Privatsphäre, gibt’s da nicht 'ne App für? - Verbesserung von Privatsphäre-relevantem Verhalten durch bessere Informationen

DIPL.-PSYCH. PAUL GERBER, GEBOREN IN HALLE / SAALE, DEUTSCHLAND

GENEHMIGTE PROMOTIONSSCHRIFT ZUR ERLANGUNG DES AKADEMISCHEN GRADES

DOCTOR RERUM NATURALIUM (DR. RER. NAT.)

AM FACHBEREICH HUMANWISSENSCHAFTEN DER TECHNISCHEN UNIVERSITÄT DARMSTADT

INSTITUT FÜR PSYCHOLOGIE

„And then some magic happens …“

(Anonym)

REFERENT:	PROF. DR. JOACHIM VOGT
CO-REFERENT:	PROF. DR. SARAH DIEFENBACH
EINREICHUNGSTERMIN:	09.10.2017
PRÜFUNGSTERMIN:	30.10.2017
ERSCHEINUNGSORT:	DARMSTADT, DEUTSCHLAND
ERSCHEINUNGSJAHR:	2017
HOCHSCHULKENNZIFFER:	D17

Promotionsschrift von Herrn Dipl.-Psych. Paul Gerber

Erklärung gemäß §9 der Allgemeinen Bestimmungen der Promotionsordnung der Technischen Universität

Hiermit versichere ich, die vorliegende Arbeit ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus den Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den .....

.....
Unterschrift

Paul Gerber

Martinstraße 26

64285 Darmstadt

Wissenschaftlicher Werdegang

Name:	Paul Gerber
Geburtsdatum:	13.11.1984
Geburtsort:	Halle / Saale, Deutschland
Familienstatus:	verheiratet

Ausbildung:

2005 – 2012	Diplom in Psychologie an der Technischen Universität Darmstadt im Fachbereich Humanwissenschaften
2004	Abitur am Kepler Gymnasium Freiburg i. Breisgau, Deutschland

Arbeitserfahrung:

Seit 2012	Wissenschaftlicher Mitarbeiter in der Forschungsgruppe Arbeits- und Ingenieurpsychologie (FAI) der Technischen Universität Darmstadt
2014 – 2017	Wissenschaftlicher Mitarbeiter in der Forschungsgruppe Security, Usability and Society (SECUSO) im Fachgebiet Informatik der Technischen Universität Darmstadt
2010 – 2012	Studentische Hilfskraft in der Forschungsgruppe für Arbeits- und Ingenieurpsychologie in den Bereichen HCI und Usability
2009 – 2010	Studentische Hilfskraft an der Technischen Universität Darmstadt in der Forschungsgruppe für Entscheidungsforschung in den Bereichen intuitive Nutzung und intuitive Entscheidung
2007 – 2010	Studentische Hilfskraft in der Hochschuldidaktischen Arbeitsstelle der Technischen Universität Darmstadt in den Bereichen Projektmanagement, Seminarleitung und -assistenz sowie Recherche und Aufbereitung von Inhalten

Inhaltsverzeichnis

Zusammenfassung

Die vorliegende Arbeit beschäftigt sich mit dem digitalen Alltag von Endanwendern und den damit verbundenen Implikationen für die individuelle Privatsphäre. Der digitale Alltag beschreibt dabei den alltäglichen Umgang mit dem Smartphone beziehungsweise digitalen Diensten im Allgemeinen und die dafür häufig notwendige Preisgabe persönlicher Daten. In diesem Kontext wird auch das sogenannte Privatsphären Paradoxon thematisiert, welches den scheinbaren Widerspruch zwischen der Einstellung zu Privatsphäre-relevantem Verhalten und tatsächlich gezeigtem Verhalten beschreibt, und mittels eines integrativen Verhaltensmodells für Privatsphäre-relevantes Verhalten mögliche Erklärungen formuliert. Die Arbeit nähert sich dem Problemkomplex zunächst explorativ und versucht ein kleineres Teilproblem zu lösen, um danach induktiv auf den daraus gewonnenen Erkenntnissen sowie dem Stand der Forschung aufbauend ein erweitertes Modell zur Beschreibung des Phänomens zu formulieren.

Für die Nutzung des Smartphones und der damit verfügbaren Online-Dienste werden im Allgemeinen kleine Softwareprogramme beziehungsweise Applikationen („Apps“) genutzt. Diese Applikationen sind, je nach verwendeten Betriebssystem, in zumeist bereits vorinstallierten Applikations-Stores zum Download verfügbar. Der Anwender kann hierbei aus mehreren Millionen verschiedenen Applikationen für die verschiedensten Anwendungsszenarien wählen. Ob für die Fahrplanauskunft des öffentlichen Nahverkehrs, ein kleines Sudoku Spiel zwischen durch oder Onlinebanking, mittels Smartphone und der zugehörigen Applikation ist dies alles unterwegs möglich. Viele Applikationen benötigen dabei Zugriff auf zum Teil persönliche Daten, die auf dem Smartphone gespeichert sind oder nutzen die vielfältigen Sensoren, die diese Geräte bieten. Dabei sind diese Daten zum Teil für die Funktionalität notwendig, wie zum Beispiel der aktuelle Aufenthaltsort bei einer Navigationssoftware, zum Teil aber auch nicht. Der Zugriff auf diese Ressourcen wird mittels sogenannter Berechtigungen vom Betriebssystem geregelt, welche der Anwender entweder vor der Installation der Applikation oder während der Nutzung bestätigen muss. Bei dieser Entscheidung ist der Anwender auf die Informationen angewiesen, die er entweder im Store selbst oder über externe Quellen, wie z.B. Foren oder öffentlich verfügbare Testseiten, finden kann.

Um herauszufinden, wie sich gute Applikationen von weniger guten am besten unterscheiden lassen, wurden in der vorliegen Arbeit zunächst Interviews mit Experten aus der IT-Forschung und Wirtschaft geführt. Auf Basis der Erkenntnisse wurden verschiedene Heuristiken formuliert an denen sich Endanwender bei der Suche und Auswahl von Applikationen orientieren können. Hierbei zeigte sich, dass der Interpretation der durch die Applikationen geforderten Berechtigungen in Hinblick auf die eigene Privatsphäre besondere Bedeutung zukommt.

Deswegen untersucht die vorliegende Arbeit im weiteren Verlauf die Darstellung dieser Berechtigungen. Hierbei werden zunächst die Darstellungen der Berechtigungen in den beiden am weitesten verbreiteten mobilen Betriebssystemen Android von Google sowie iOS von Apple untersucht und in Hinblick auf die Nützlichkeit für die Bewertung möglicher Privatsphäre-Risiken bewertet. Es zeigen sich dabei Mängel sowohl in Bezug auf den Detailgrad als auch die Verständlichkeit der Darstellungen. Dies resultiert vor allem aus dem Bestreben durch Reduktion der Komplexität die Verständlichkeit der Darstellung zu verbessern, da dies auch ein Verlust von Informationsgehalt zur Folge hat. Vor diesem Hintergrund werden im Folgenden verschiedene Vorschläge aus der Forschungsliteratur diskutiert und auf Basis der gewonnenen Erkenntnisse Anforderungen für eine eigene Darstellung formuliert.

Auf Basis dieser Anforderungen wird im Rahmen dieser Arbeit der Prototyp einer eigenen Darstellung für Berechtigungen entwickelt und in einer Evaluationsstudie sowohl mit etablierten Darstellungen als auch Vorschlägen aus der Literatur verglichen. Es zeigt sich, dass insbesondere bei bewusster Ausnutzung des Berechtigungssystems, d.h. gezieltem Anfordern bestimmter Berechtigungsmuster, die bestehenden Darstellungen dem Endanwender keine Privatsphäre-schützende Entscheidung ermöglichen. Die Reduktion der Komplexität und der damit einhergehende Verlust an Informationsqualität kann ein Verständnis für die angeforderte Berechtigungskombination verhindern, sodass Anwender einer bewussten Täuschung hilflos ausgeliefert sind. Der entwickelte Prototyp zeigt auch in solchen Situationen eine robuste und konstant gute Informationsqualität und ermöglicht dem Anwender eine bessere Entscheidung durch bessere Informationen.

Zum besseren Verständnis der gewonnenen Erkenntnisse und um eine Übertragung auf einen allgemeinen Anwendungskontext zu ermöglichen, wird in der vorliegenden Arbeit im weiteren Verlauf ein integratives Verhaltensmodell formuliert und evaluiert. Hierbei werden insgesamt neunzehn verschiedene Einflussfaktoren, die bereits in der Literatur vorgeschlagen wurden zu einem integrativen Verhaltensmodell zusammengefügt und in einer Onlinestudie zur Verhaltensvorhersage genutzt. Die Teilnehmer werden hierbei zunächst nach verschiedensten persönlichen Informationen befragt, um in der zweiten Phase der Studie Fragen zu den erhobenen Konstrukten zu beantworten.

Hierbei kristallisieren sich insbesondere die situationsspezifischen Privatsphäre-Bedenken, die subjektiven Vorteile der Dienstnutzung sowie die subjektive Sensitivität der abgefragten Daten als gute Prädiktoren mit direkten Effekten auf das gezeigte Verhalten heraus. Es zeigt sich, dass eine umfassendere Betrachtung der diversen Einflussfaktoren helfen kann, die Verhaltensbildung im Kontext der Privatsphäre besser zu verstehen. In den letzten zehn Jahren wurde in der Privatsphären-Forschung häufig ein Mangel an Verständnis und Bewusstsein gegenüber technischen Vorgängen und Zusammenhängen bei Endanwendern dokumentiert, wobei hierbei sowohl Usability-Probleme als auch fehlendes Wissen oder Aufmerksamkeit als mögliche Ursachen diskutiert und identifiziert wurden. Die Ergebnisse unterstreichen dabei die Bedeutsamkeit dieser Erkenntnisse. Anwender berücksichtigen in ihren Entscheidungen durchaus in starkem Maße, ob erhobene Daten eine Verletzung der eigenen Privatsphäre darstellen. Um dies jedoch zu tun müssen sie dafür wissen, welche Daten überhaupt erhoben werden und, insbesondere bei eher technischen Daten wie z.B. IP-Adressen, was diese bedeuten. Der Gestaltung gut strukturierter Informationen kommt somit im Kontext der Privatsphäre besondere Bedeutung zu, da nur diese den Anwender in die Lage versetzen in seinem Sinne gute und fundierte Entscheidungen zu treffen.

Abstract

The present work deals with the digital everyday life of end users and the implications for individual privacy. Digital everyday life describes the everyday use of smartphones and digital services in general and the often necessary disclosure of personal data. In this context, the so-called privacy paradox is also addressed, which describes the apparent contradiction between attitudes towards behavior relevant to privacy and actually shown behavior, and formulates possible explanations by means of an integrative behavioral model for behavior relevant to privacy. The work approaches the thematic complex exploratively and tries to solve a smaller sub-problem, in order to formulate an extended model for the description of the phenomenon inductively based on the findings and the state of research.

To use the smartphone to its full extent, small applications ("Apps") are generally necessary. Depending on the operating system used, these applications are usually available for download in pre-installed application stores. The user can choose from several million different applications for a wide variety of application scenarios. Whether for public transport timetable information, a small Sudoku game between through or online banking, this is all possible on the road using a smartphone and the associated application. Many applications require access to some personal data stored on the smartphone or use the various sensors offered by these devices. In some cases, this data is necessary for the functionality, such as the current location in a navigation software, but sometimes it is not. Access to these resources is controlled by the operating system by means of so-called permissions, which the user must confirm either before installing the application or during use. In making this decision, the user relies on information that can be found either in the store itself or through external sources, such as forums or publicly available test sites.

In order to find out how best to distinguish good applications from less good ones, interviews with experts from IT research and industry were conducted in the present work. Based on the findings, various heuristics have been formulated to guide end users in the search and selection of applications. It became clear that the interpretation of the permissions requested by the applications is of particular importance with regard to the users' own privacy.

For this reason, the present work examines the representation of these permissions in the further course of this work. The first step is to examine the interfaces of the permissions in the two most widely used mobile operating systems, Google's Android and Apple's iOS, and to assess their usefulness for evaluating potential privacy risks. There are deficiencies in terms of both the level of detail and the comprehensibility of the interfaces. This is mainly due to the effort to reduce complexity in order to improve the comprehensibility of the presentation, as this also results in a loss of information content. Against this background, various proposals from the research literature will be discussed in the following and, based on the findings gained, requirements for an interface will be formulated.

Based on these requirements, the prototype of an own interface for permissions is developed and compared in an evaluation study with established interfaces as well as proposals from the literature. It is shown that especially in the case of deliberate exploitation of the permission system, i. e. targeted requesting of certain permission patterns, the existing interfaces do not allow the end user to make a decision that protects privacy. The reduction of complexity and the associated loss of information quality can prevent an understanding of the required combination of permissions, so that users are

helplessly at the mercy of deliberate deception. The developed prototype shows a robust and constantly good quality of information even in such situations and enables the user to make a better decision through better information.

In order to better understand the insights gained and to enable a transfer to a more general application context, an integrative behavioral model will be formulated and evaluated in the course of this work. In this context, a total of nineteen different influencing factors, which have already been suggested in the literature, are combined to form an integrative behavioral model and used in an online study for behavioral prediction. Participants are first asked for various personal information. In the second phase of the study they are then asked to answer questions about the influencing factors.

In this context, the situation-specific privacy concerns, the subjective advantages of service use and the subjective sensitivity of the queried data emerge as good predictors with direct effects on the behaviour shown. It has been shown that a more comprehensive examination of the various influencing factors can help to better understand behavioral formation in the context of privacy. In the last ten years, privacy research has often documented a lack of understanding and awareness of technical processes among end users, whereby usability problems as well as lack of knowledge or attention have been discussed and identified as possible causes. The results underline the significance of these findings. Users take into account to a large extent whether the data collected constitutes a violation of their own privacy. In order to do this, however, they need to know which data is collected at all and, especially in the case of more technical data such as IP addresses, what they mean. The design of well-structured information is therefore particularly important in the context of privacy, as only this enables the user to make good and well-founded decisions in his or her interest.

1. Einleitung

1.1. Der digitale Alltag

Das mobile Internet ist heute, im Jahr 2017, aus unserem Alltag nicht mehr wegzudenken. Seine explosionsartige Verbreitung, insbesondere beim Endanwender, begann mit der Vorstellung des iPhone 1 im Januar 2007 durch Apple Inc.[1]. Das iPhone 1 (vgl. Abbildung 1b[2]) war zwar nicht das erste Smartphone[3], dieser Titel gebührt eher dem Nokia 9000 Communicator aus dem Jahr 1996 (vgl. Abbildung 1a[4]), jedoch war es das erste, welches weltweite Verbreitung erreichte und damit den Startschuss für die breite Nutzung des mobilen Internets durch den Endanwender gab.

Heute ist das Smartphone für viele Menschen nicht mehr aus dem Alltag wegzudenken. Aktuell verfügen deutlich über zwei Milliarden Menschen weltweit über ein Smartphone[5], vorwiegend ausgestattet mit dem Betriebssystem Android[6]. Die (fast) unbegrenzte Verfügbarkeit des Internets führte in den vergangenen zehn Jahren zu einer Veränderung im Internet-Nutzungsverhalten sowie zu einem rapide wachsenden Angebot an neuen mobilen Diensten. Insbesondere die Nutzung sozialer Netzwerk wie Facebook[7] oder Twitter[8] zur Vernetzung mit der Familie, mit Freunden, Bekannten aber auch einfach nur Menschen mit ähnlichen Interessen oder anderen Gemeinsamkeiten hat zugenommen [1], [2]. Viele Menschen haben heute eine oder gar mehrere digitale Repräsentationen, „digitale Ichs“, die sie pflegen. Aber auch andere Dienste, z.B. die Navigation mittels verschiedener digitaler Kartenangebote oder auch das Einkaufen in Onlineshops sind mittels Smartphone dank des bequemen Zugriffs von (fast) überall Teil des Alltags vieler Menschen geworden. Der Austausch von Daten (Bild, Ton, Schrift, …) in Sekunden mit (fast) beliebig vielen Menschen an beliebigen Orten der Welt war nie zuvor so einfach.

Abbildung 1. (A) Der Nokia Communicator 9000 aus dem Jahr 1996 (B) Das iPhone der ersten Generation aus dem Jahr 2007

[1] http://www.tagesspiegel.de/wirtschaft/10-jahre-iphone-das-erste-smartphone-war-ein-nokia/19221898.html ; letzter Abruf 04.10.2017

[2] Originalaufnahme des Benutzers „Carl Berkeley“ (https://www.flickr.com/people/38455623@N05) unter der Lizenz „Attribution-NoDerivs 2.0 Generic“ - https://creativecommons.org/licenses/by-nd/2.0/legalcode

[3] mobile Telefone, die darüber hinaus die Funktionalitäten weiterer Geräte erfüllen, wie z.B. Navigation, mobiler Internetzugang, Terminplanung, E-Mail etc.

[4] Originalaufnahme des Benutzers „textlad“ (https://www.flickr.com/photos/textlad/) unter der Lizenz „Attribution 2.0 Generic“ - https://creativecommons.org/licenses/by/2.0/legalcode

[5] https://de.statista.com/statistik/daten/studie/309656/umfrage/prognose-zur-anzahl-der-smartphone-nutzer-weltweit/ ; letzter Abruf 04.10.2017

[6] https://de.statista.com/statistik/daten/studie/246004/umfrage/weltweiter-bestand-an-smartphones-nach-betriebssystem/ ; letzter Abruf 04.10.2017

[7] www.facebook.com

[8] www.twitter.com

Zur Bereitstellung vieler dieser Dienste werden sogenannte Applikationen genutzt, welche auf dem Smartphone installiert werden müssen. Diese benötigen, je nach angebotener Funktionalität, jedoch persönliche Daten in verschiedenem Maße und in unterschiedlicher Ausprägung. So ist es leicht nachvollziehbar, dass eine zielführende Navigation von zu Hause bis zum Urlaubshotel nur möglich ist, wenn das jeweilige Gerät die aktuelle Position erfassen kann. Soweit das Kartenmaterial nicht auf dem Gerät selbst vorliegt, wie es z.B. bei GoogleMaps[9] der Fall ist, muss diese Position auch einem entfernten Sever zur Verfügung gestellt werden, sodass er diese mit dem Kartenmaterial abgleichen und eine Route vorschlagen kann.

Darüber hinaus sammeln viele Applikationen aber auch Daten, welche nicht zwingend notwendig für die Bereitstellung der Funktionalität sind [3]. Die so gesammelten Daten können somit, über die Bereitstellung des gewünschten Dienstes hinaus, potentiell auch für weitere Zwecke genutzt werden. Hierunter fällt beispielsweise die Erstellung eines Anwenderprofils, auf Basis dessen unter Verwendung sogenannter Big Data-Analysen Aussagen über Verhalten in den eigenen vier Wänden, über persönliche Wünsche und Vorlieben oder beispielsweise auch die politische Einstellung getroffen werden können. Es ist somit im digitalen Alltag dank des Smartphones und der damit erfassbaren Daten möglich, ohne die explizite und absichtliche Beobachtung einer einzelnen Person personenbezogene Aussagen über diese Person zu treffen, auch wenn dies subjektiv ihre individuelle Privatsphäre verletzen sollte.

1.2. Was ist eigentlich Privatsphäre?

In der Forschung gibt es zwei große Strömungen zur Definition von Privatsphäre. Die eine betrachtet Privatsphäre als Wert, der sowohl gesellschaftlicher als auch persönlicher Natur sein kann [4]. Informationen werden also gegen wahrgenommene Vorteile getauscht. Hier runter können beispielsweise Serviceleistungen, Funktionen oder Rabatte fallen. Die zweite Strömung betrachtet Privatsphäre als einen aktuellen Zustand. Westin [5] beschreibt hierbei vier voneinander zu unterscheidende Privatsphären-Zustände:

1. Abgeschiedenheit (Freisein von Beobachtungen)
2. Vertraulichkeit (Bilden von kleinen Gruppen, in denen enge, entspannte und aufrichtige Verbindungen möglich sind)
3. Anonymität (Freiheit von Identifikation und Überwachung)
4. Zurückhaltung (Limitieren von Offenlegung gegenüber anderen)

Aufbauend darauf wird Privatsphäre als „Zustand mit beschränktem Zugriff auf eine Person“ definiert [6], was sich im weiteren Verlauf der Forschung, insbesondere im digitalen Kontext, zu einem „beschränkten Zugriff auf (persönliche) Informationen“ entwickelte [7]. Ein entscheidender Faktor hierbei ist die Möglichkeit der Kontrolle über die Umstände und Bedingungen, unter denen persönliche Informationen durch Dritte erfasst und verarbeitet werden [8]. Insofern kann die individuelle Privatsphäre (oder auch die Verletzung derselben) nicht schlicht am Teilen oder Speichern verschiedener Informationen festgemacht werden. Besteht beispielsweise ein Zustand der Vertraulichkeit (vgl. Westin oben) oder auch Anonymität, ist es einfach nachvollziehbar, dass bereitwilliger persönliche Informationen weitergegeben werden, als wenn dies nicht der Fall ist. Das gleiche gilt für den Fall, dass die Informationen mit Zustimmung gesammelt werden.

[9] www.google.de/maps

1.3. Das Privatsphären Paradoxon

Betrachtet man das Problem der Privatsphäre im Kontext des digitalen Alltags, trifft man schnell auf das Phänomen des sogenannten Privatsphären Paradoxons [9], [10]. Dieses beschreibt eine Diskrepanz zwischen der Einstellung gegenüber einer bestimmten Privatsphäre-relevanten Handlung und dem tatsächlich gezeigten Verhalten. So äußern Nutzer häufig Bedenken und zeigen eine negative Einstellung bezüglich der Datensammlung durch Applikationen auf Smartphones oder in sozialen Netzen, gleichzeitig verhalten sie sich aber auf eine Weise, die dieser Einstellung scheinbar widerspricht [7], [9], [11], [12]. Einerseits werden freiwillig Daten preisgegeben, indem z.B. bestimmte Aspekte des eigenen Privatlebens in sozialen Netzwerken geteilt oder Fitness-Tracker und Onlineshopping-Websites mit Profiling-Funktionen genutzt werden. Andererseits wird wenig aktive Mühe betrieben, die eigenen Daten zu schützen. Begründungen für diesen scheinbaren Widerspruch werden in der Literatur verschiedenste angeführt. Häufig genannte Gründe sind das fehlende Bewusstsein für entweder die Sammlung von persönlichen Daten und/oder die daraus möglicherweise folgenden Konsequenzen [13–15], d.h. die mit der Weitergabe verbundenen Risiken. Anwender wünschen sich häufig mehr Transparenz und Kontrolle über die Frei- und Weitergabe von persönlichen Daten [16]. Einen sehr guten und umfassenden Überblick über weitere Erklärungsansätze bietet beispielsweise [10].

1.4. Problemstellung und Ziele der Arbeit

Im Zentrum des digitalen Alltags steht das private Mobilgerät, zumeist ein Smartphone oder Tablet, dessen Funktionen bzw. dessen Nutzen primär durch die Art und Menge der genutzten Applikationen definiert wird. Der Auswahl der passenden Applikation kommt also sowohl für die optimale Nutzung als auch für den Schutz der eigenen Privatsphäre zentrale Bedeutung zu.

Für den Anwender bestehen dabei verschiedene Probleme hinsichtlich der Nutzung und Auswahl von Applikationen für sein Smartphone. Einer möglichst informierten Entscheidung darüber, welche Applikation für den gegebenen Anwendungsfall und den individuellen Nutzer am besten geeignet ist, stehen primär die Intransparenz der Entscheidungssituation, insbesondere in Hinblick auf die Art und Angemessenheit der gesammelten Daten sowie ein fehlendes Bewusstsein für die Möglichkeit der Datensammlung an sich gegenüber [17–20].

Entsprechend ist das vordergründige Ziel der vorliegenden Arbeit die Entwicklung eines Interface Prototypens bzw. einer Erweiterung eines bestehenden Interfaces, welches möglichst informierte Entscheidungen bei der Smartphone-Nutzung (im Speziellen bei der Auswahl von Applikationen) in Hinblick auf die eigene Privatsphäre unterstützt. Eine Entscheidung ist hierbei dann eine informierte Entscheidung in Hinblick auf die Privatsphäre, wenn der Anwender sich über mögliche Datenzugriffe und -weitergabe durch eine zu installierende Applikation bewusst ist und sich unter Berücksichtigung dieses Wissens entschieden hat. Das bedeutet nicht zwangsläufig, dass er sich in jedem Fall für die Privatsphäre-freundlichste Alternative entscheiden muss, solange für ihn mögliche Vorteile der von ihm getroffenen Wahl überwiegen und er sich der möglichen Nachteile bewusst ist.

Um die dadurch gewonnenen Erkenntnisse zu erweitern und weiter generalisieren zu können, ist die Formulierung eines integrativen Verhaltensmodells ein nachgelagertes Ziel der vorliegenden Arbeit. Unter einem integrativen Verhaltensmodell wird dabei ein Modell verstanden, welches die im Rahmen der Entwicklung des Prototypens sowie im Zuge von Literaturrecherchen vorgefundenen

einzelnen Faktoren so strukturiert, dass Zusammenhänge zwischen den einzelnen Faktoren erkennbar werden. Darüber hinaus wird eine Gewichtung der verhaltensbildenden Faktoren angestrebt, sodass besonders bedeutsame und weniger bedeutsame Faktoren identifiziert werden können.

Die Arbeit folgt hierbei dem Ansatz, sich zunächst explorativ dem Themenfeld zu nähern und ein kleineres Teilproblem zu lösen. Induktiv auf den daraus gewonnenen Erkenntnissen sowie dem Stand der Forschung in der Literatur aufbauend wird dann ein erweitertes Modell zur Beschreibung des Phänomens formuliert und geprüft. Somit werden folgende Zwischenziele und untergeordnete Fragestellungen in dieser Arbeit definiert:

1. Probleme und Schutzmöglichkeiten des digitalen Alltags, im Speziellen bei der Nutzung eines Smartphones, kennen
    a. Wie entscheiden (Privacy)Experten bei der Nutzung von Smartphones, welche Applikationen empfehlenswert sind? [17] - Kapitel 2.1 ab Seite 13
    b. Welche Zugriffsberechtigungssysteme sind im mobilen Kontext zu betrachten? [21] – Kapitel 2.2 ab Seite 18
    c. Welche Empfehlungen und Alternativen wurden bereits in der Forschungsliteratur vorgestellt? [22] – Kapitel 2.3 ab Seite 24
    d. Welche Anforderungen an ein verbessertes Interface lassen sich daraus ableiten? – Kapitel 2.3.1 ab Seite 27
2. Entwicklung eines Prototypen Interfaces, zur Verbesserung der Informationslage von Endanwendern bei der Applikationsauswahl
    a. Evaluation und Vergleich sowohl mit Ist-Stand als auch Empfehlungen bzw. Alternativen auf Basis der Literatur [22] – Kapitel 3 ab Seite 29
3. Formulieren eines integrativen Verhaltensmodells für Privatsphäre-relevantes Verhalten
    a. Identifikation relevanter Einflussfaktoren für menschliches Handeln auf Basis des Standes der Forschung und der Ergebnisse der empirischen Betrachtung der App-Auswahl und Aufstellen des integrativen Verhaltensmodells – Kapitel 4.2 ab Seite 50
    b. Hypothesengeleitetes Prüfen der Passung des theoretischen Verhaltensmodells – Kapitel 4.3 ab Seite 59

Die referenzierten Publikationen entsprechen hierbei jenen, deren Inhalte für die Erreichung des jeweiligen Zwischenziels maßgeblich waren und an denen der Autor der vorliegenden Arbeit beteiligt war und welche somit maßgeblicher Bestandteil dieser Arbeit sind. Die Inhalte werden im Kontext dieser Arbeit sinnvoll zusammengefasst und eingeordnet. Die Originalversionen der Publikationen sind alle online verfügbar.

1.5. Struktur der weiteren Arbeit

Der Aufbau der vorliegenden Arbeit folgt den oben genannten Zwischenzielen. In Kapitel 2 werden die für eine Entscheidung für oder gegen eine Smartphone Applikation notwendigen Informationen beschrieben. Es wird auch darauf eingegangen, wie diese Informationen für den Anwender dargestellt werden können, sowohl aus Sicht der Praxis als auch der Forschung. In Kapitel 3 wird eine prototypische Darstellung für Berechtigungen im Detail beschrieben und eine zugehörige Evaluationsstudie vorgestellt. In Kapitel 4 wird auf Basis des Literaturkörpers und der empirischen Erkenntnisse aus den vorherigen Kapiteln ein integratives Verhaltensmodell formuliert und evaluiert.

In Kapitel 2 wird hierfür zunächst in Unterkapitel 2.1 eine Studie zum Vorgehen von Privatsphäre-Experten bei der Auswahl von Applikationen für das Smartphone und die darauf basierende Formulierung von Handlungsempfehlungen bzw. Heuristiken vorgestellt. In Unterkapitel 2.2 werden die Darstellungen von Berechtigungen in Android (Google) und iOS (Apple) in verschiedenen Versionen beschrieben und diskutiert. Danach werden in Unterkapitel 2.3 Vorschläge anderer Forscher diskutiert und daraus folgend Anforderungen an eine eigene Darstellung formuliert.

In Kapitel 3 wird zunächst im Unterkapitel 3.1 der entwickelte Prototyp beschrieben. Das Unterkapitel 3.2 geht im Anschluss detailliert auf die durchgeführte Evaluationsstudie ein und diskutiert die Ergebnisse im Forschungskontext anderer Arbeiten. Unterkapitel 3.3 führt die bisherigen Erkenntnisse zusammen, formuliert noch bestehende Lücken und leitet das weitere Vorgehen ab.

In Kapitel 4 wird zu Beginn ein kurzer Abriss zu klassisch psychologischen Verhaltenstheorien gegeben, bevor in Unterkapitel 4.1 kurz die Methodik der Literaturrecherche skizziert wird. Danach werden in Unterkapitel 4.2 auf Basis des aktuellen Standes der Literatur sowie den in den vorherigen Kapiteln vorgestellten empirischen Erkenntnissen verhaltensbildende Faktoren gesammelt und ein integratives Verhaltensmodell der Einflussfaktoren für menschliches Verhalten im digitalen Alltag formuliert. Im Anschluss daran wird in Unterkapitel 4.3 die empirische Überprüfung des Modells im Detail beschrieben. Unterkapitel 4.4 schließt das Kapitel mit einer Diskussion der Erkenntnisse sowie einer Betrachtung der Implikationen für Praxis und Forschung.

Die Arbeit schließt in Kapitel 5 mit einer zusammenfassenden Betrachtung der Erkenntnisse, einer Überprüfung der Zielerreichung sowie einem Ausblick auf zukünftige Arbeiten.

2. Probleme und Schutzmöglichkeiten im digitalen Alltag

Ein modernes Smartphone, über welches aktuell mehr als zwei Milliarden Menschen weltweit verfügen[10] bietet eine Vielzahl von Funktionen. Ob es um die Navigation, das durch unsere Stimme gesteuerte Eintragen von Terminen, das Einkaufen von unterwegs oder das einfache Telefonieren geht, für all dies benötigt man heutzutage nur noch ein Smartphone.

All diese Funktionen werden durch kleine Programme zur Verfügung gestellt, die Applikationen oder kurz „Apps" genannt werden. Diese benötigen hierfür von uns verschiedene Informationen, von der Eingabe von Zugangspasswörtern, um sich beim Online-Shop seiner Wahl anzumelden bis hin zu unserem persönlichen Kalender, um dort Termine für uns zu vermerken oder uns daran zu erinnern.

Beim Kauf eines Smartphones ist normalerweise bereits eine Auswahl von Applikationen installiert, z.B. ein Browser oder auch eine E-Mail-Applikation. Aber nicht für jeden Zweck ist bereits etwas installiert und selbst wenn bietet die vorinstallierte Applikation möglicherweise nicht alle Funktionen, die der Anwender möchte oder ist nicht optimal zu bedienen. Deshalb gibt es sogenannte Applikations-Stores, die ebenfalls normalerweise bereits vorinstalliert sind und direkt genutzt werden können. Unter Android ist es der „Play Store", Apple nennt ihn schlicht „App Store". Neben diesen offiziellen Stores gibt es noch eine Vielzahl weiterer, die ebenfalls genutzt werden können, aber zumeist ein deutlich kleineres oder in manchen Fällen auch spezielleres Angebot haben. Hierzu gehört z.B. der F-Droid Store[11], welcher ausschließlich Open-Source Applikationen anbietet.

In diesen Stores stehen diverse Informationen über die verschiedenen Applikationen bereit, um dem suchenden Anwender die Auswahl zu erleichtern. Neben obligatorischen Informationen, wie dem Namen, Logo, dem Entwickler und einer funktionalen Beschreibung einer Applikation, stehen ggf. auch Screenshots oder Videos zur Verfügung. Zusätzlich werden häufig auch Downloadzahlen, Bewertungen und Review-Texte durch Anwender sowie Informationen über die letzten Updates durch den Entwickler sowie die vom Entwickler vorgesehenen Zugriffsberechtigungen zur Verfügung gestellt. Letztere regeln in mobilen Betriebssystemen die Zugriffe auf Telefonfunktionen (z.B. WLan oder die verschiedenen Sensoren) sowie auf die auf dem Gerät gespeicherten Daten und Informationen (z.B. Kontakte oder Fotos). Sie sind also ein essentieller Schutzmechanismus innerhalb des Betriebssystems.

Auf Basis dieser Informationen können Anwender sich für oder gegen eine Applikation entscheiden. Doch was gilt es hierbei für eine sinnvolle Auswahl zu beachten? Wie sollte man vorgehen und gibt es darüber hinaus noch andere Informationen die bei der Auswahl berücksichtig werden sollten? Des Weiteren stellt sich die Frage, wie diese Informationen in den verschiedenen Stores für den Anwender aufbereitet sind. Aus den Antworten auf diese Frage schließlich leitet sich der Bedarf oder ggf. auch fehlender Bedarf einer Intervention zur Verbesserung der Entscheidungsqualität für Anwender ab.

Insofern werden für das aktuelle Kapitel folgende Ziele formuliert:

1. Formulierung von Heuristiken[12] für Endanwender zur besseren, d.h. Privatsphäre-schützenden Wahl von Applikationen

[10] https://de.statista.com/statistik/daten/studie/309656/umfrage/prognose-zur-anzahl-der-smartphone-nutzer-weltweit/ ; letzter Abruf 04.10.2017

[11] https://f-droid.org/

[12] Unter Heuristiken werden hierbei Regeln zum Problemlösen verstanden, die auch unter Informationsmangel in komplexen Situationen häufig zu guten Lösungen führen und dennoch effizient anwendbar sind

2. Überblick über aktuelle Berechtigungsinterfaces im mobilen Kontext
3. Überblick über alternative Berechtigungsdarstellungen aus der Forschung
4. Ableiten von Anforderungen an eine Intervention

Das vorliegende Kapitel ist, diesen Zielen folgend, so strukturiert, dass zunächst betrachtet wird, nach welchen Heuristiken Endanwender sinnvollerweise Applikationen für ihr Smartphone wählen sollten und wie diese aufgestellt wurden. Im Anschluss daran wird ein Überblick über die zum Zeitpunkt der Arbeit aktuellen Berechtigungssysteme (basierend auf den weltweiten Marktanteilen) im mobilen Kontext gegeben. Abschließend werden auch bereits in der Literatur vorgeschlagene Alternativen zu den bestehenden Berechtigungsinterfaces beschrieben und darauf aufbauend Anforderungen an eine verbesserte Version formuliert.

2.1. Heuristiken für die Privatsphäre-orientierte Auswahl von Smartphone Applikationen

In diesem Kapitel wird eine Studie im Detail beschrieben, in welcher IT-Experten dazu befragt wurden, wie sie selbst Applikationen auswählen und was sie Endanwendern hierzu raten würden. Auf Basis dieser Empfehlungen wurden Heuristiken für den Endanwender formuliert, die sich insgesamt in vier Bereiche einteilen lassen. Zum Abschluss des Kapitels werden diese Heuristiken mit bestehenden Stores für Smartphone Applikationen verglichen und geprüft, ob und an welcher Stelle eine Intervention zur Verbesserung der Applikationswahl sinnvoll erscheint.

Im Folgenden werden zunächst die Inhalte des Interviews sowie der Auswertungsvorgang, danach die Zusammensetzung und Rekrutierung der Stichprobe kurz zusammengefasst. Danach werden die Ergebnisse in Form der gefundenen Heuristiken dargestellt. Eine detaillierte Beschreibung der Studie findet sich in [17].

2.1.1. Studiendesign und Auswertung

Zur Identifikation der Heuristiken von Experten wurden teilstrukturierte Interviews durchgeführt, welche etwa eine Stunde dauerten. Inhalt der Interviews waren neben der Erfassung der persönlichen Erfahrungen im IT Kontext v.a. auch die Durchführung zweier Applikationssuchen unter Verwendung der Think-Aloud-Methode[13] sowie die Formulierung von persönlichen Empfehlungen für den Endanwender in Bezug auf die Applikationswahl. Der vollständige Interviewleitfaden findet sich im Anhang ab Seite 84 dieser Arbeit.

Alle Interviews wurden vollständig transkribiert und mit einer offenen Kodierung durch mindestens zwei der beteiligten Autoren versehen. Bei der Kodierung wurde primär das Ziel verfolgt, Heuristiken zu identifizieren, nach denen die Teilnehmer bei der Applikationssuche und -auswahl vorgehen oder welche sie Endanwendern empfehlen würden. Die Kodierungsliste wurde zunächst durch jeden Autor einzeln erstellt und im Anschluss mit allen Autoren diskutiert und eine gemeinsame vollständige Liste formuliert. Im Anschluss wurden alle Kategorien mit passenden Zitaten aus den Interviews verknüpft. Da das Ziel die Formulierung von Heuristiken für die Auswahl von Privatsphäre-schützenden Applikationen war, wurden solche ausgeklammert, die sich z.B. mit der Farbe des Interfaces

[13] Das bedeutet, dass die Teilnehmer während der Suche nach einer ihrer Meinung nach passenden Applikation ihr Gedanken verbalisieren sollten, sodass sie durch die Versuchsleitung nachvollzogen und dokumentiert werden können

beschäftigten. Die Anzahl der Nennungen der verschiedenen Heuristiken wurde nicht gezählt, da eine qualitative und möglichst vollständige Liste möglicher Heuristiken das Ziel war.

2.1.2. Stichprobe und Rekrutierung

Es wurden insgesamt 26 Experten interviewt, welche alle ein Informatik-nahes Betätigungsfeld hatten. Von den befragten Experten arbeiteten darüber hinaus neunzehn explizit im Feld der IT-Security, u.a. im Bereich Kryptographie sowie Android Sicherheit. Es wurden insgesamt fünf Studierende, dreizehn Doktoranden, fünf Postdoktoranden im Forschungsbereich, ein Postdoktorand aus der Industrie sowie zwei Professoren befragt. Insgesamt nahmen sechs Frauen sowie 20 Männer an der Studie teil. Siebzehn benutzen selbst ein Android basiertes Smartphone, acht ein iPhone und einer ein Smartphone mit Windows-Phone Betriebssystem.

Die Rekrutierung lief mittels Schneeball-System ab. Es wurden ausschließlich informatiknahe Interviewteilnehmer rekrutiert. Hierfür wurden sowohl Mailverteiler an der Universität genutzt sowie Kollegen der beteiligten Autoren rekrutiert. Die Teilnahme wurde nicht vergütet.

2.1.3. Abgeleitete Heuristiken

Es konnten insgesamt 15 Heuristiken identifiziert werden, welche sich insgesamt vier Kategorien zuordnen ließen. Diese Kategorien sollen im Folgenden skizziert und die eingeordneten Heuristiken genannt und beschrieben werden. Zur Verdeutlichung wird auch jeweils ein passendes Zitat aus den Transkripten der Interviews (in kursiver Schrift) angeführt. Weitere Zitate und mehr Details finden sich in der originalen Veröffentlichung zur Studie [17]. Einen Überblick über die gefundene Struktur der Heuristiken bietet Abbildung 2.

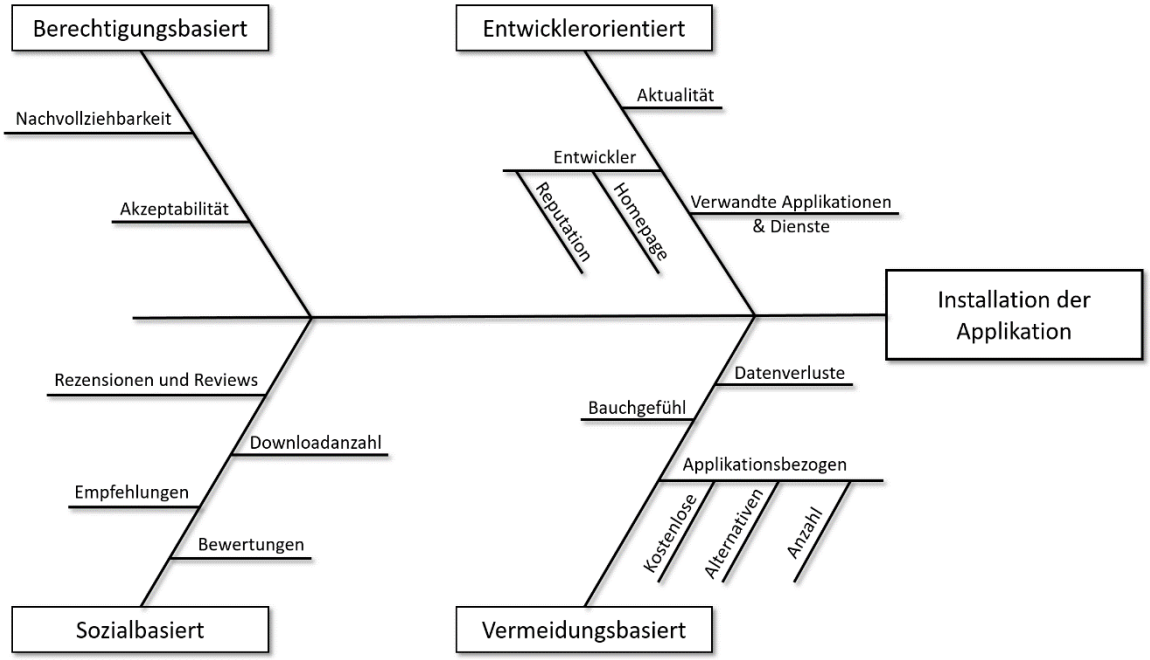

Abbildung 2. Überblick zur Struktur der Heuristiken für ein Privatsphäre-orientierte Auswahl von Smartphone Applikationen

2.1.3.1. Berechtigungsbasierte Heuristiken

In diese Kategorie fallen alle Heuristiken, welche sich mit den Zugriffsberechtigungen auf bestimmten Daten der fraglichen Applikation beschäftigen. Hierunter fallen insgesamt zwei Heuristiken, zum einen, ob die geforderten Berechtigungen nachvollziehbar, zum anderen ob diese akzeptabel sind.

Bei der erstgenannten Heuristik gilt es zu bewerten, ob die angeforderten Zugriffsberechtigungen für den angestrebten Zweck bzw. die gebotene Funktionalität der Applikation sinnhaft sind. Das bedeutet, dass bewertet werden soll, ob sie notwendig für die Erfüllung der Funktionalität sind oder nicht. Im Kontext der Studie trifft das beispielsweise für den Zugriff auf die gespeicherten Fotos durch eine Fotobearbeitungsapplikation zu, jedoch nicht für einen Zugriff auf beispielsweise die Kontakte.

> *„Eine Foto-Bearbeitungs-App benötigt Zugriff auf meine Fotos, damit sie korrekt arbeiten kann." (Proband 7)*

In Hinblick darauf, ob eine angeforderte Berechtigung auch akzeptabel ist, hängt die Beurteilung von verschiedenen Aspekten ab. Teilnehmer nannten u.a. eigene Mechanismen, um Zugriffe trotz gewährter Berechtigung zu blockieren, oder eine Applikation nur einen begrenzten, kurzen Zeitraum zu nutzen und sie danach zu schließen oder gar direkt wieder zu deinstallieren als Faktoren, die sie bei dieser Beurteilung berücksichtigen. Auch Informationen, die bereits aus anderen öffentlich zugänglichen Quellen erschlossen werden können, galten als eher akzeptabel.

> *„Da man auch auf vielen anderen Wegen herausfinden kann, dass ich in [anonymisiert] arbeite, macht es keinen großen Unterschied, ob die App meine Position kennt oder nicht." (Proband 5)*

2.1.3.2. Entwicklerorientierte Heuristiken

In diese Kategorien fallen Heuristiken, die sich direkt oder indirekt mit dem Entwickler der Applikation beschäftigen. Hierbei wurden verschiedene Kriterien genannt, die bei der Bewertung des Entwicklers bzw. dessen Vertrauenswürdigkeit eine Rolle spielen. Zum einen die öffentliche Reputation eines Entwicklers, die Entwickler-Homepage und deren Inhalte bzw. Struktur, zum anderen die Regelmäßigkeit von Updates für die fragliche Applikation sowie andere, ebenfalls durch den gleichen Entwickler angebotene Applikationen oder Dienste.

In Bezug auf die Reputation wurden vor allem die Sichtbarkeit bzw. die Größe der jeweiligen Firma sowie die Länge der Existenz einer bestimmten Marke und damit verbunden ihr subjektiver Wert für den Entwickler genannt. Dahinter stand für die Teilnehmer zunächst die Annahme, dass eine große und etablierte Firma es sich nicht leisten könne, bewusst Schadsoftware zu verbreiten, da ein guter Ruf ein wertvolles aber auch zerbrechliches Gut darstellt.

> *„… bekannte Firmen können es sich nicht erlauben, absichtlich Malware mit ihren Apps zu verbreiten. Das würde sie ruinieren." (Proband 9)*

Die Homepage eines Entwicklers bietet idealerweise sowohl objektive Informationen zu der fraglichen Applikation in Form von Handbüchern, Tutorials oder Datenschutzbestimmungen als auch eher subjektive Informationen über beispielsweise Servicequalität. Einige Teilnehmer gaben auch an, dass sie eine qualitativ schlechte Homepage mit eher qualitativ schlechten Applikationen verbinden.

Insbesondere die Existenz sowie der Inhalt der Datenschutzbestimmungen, auch wenn keine Daten erhoben werden, gilt als wichtiges Kriterium.

> *„Wenn sie nicht über den Datenschutz und meine Privatsphäre schreiben, würde ich die App nicht weiter beachten. Wenn sie dort seltsames schreiben, würde ich sie ebenfalls nicht weiter beachten. Selbst wenn sie gar nichts sammeln, sollten sie sich dennoch die Mühe machen und einen Satz wie ‚Wir sammeln keine Daten' hinschreiben und alles ist gut. Wenn sie das nicht machen, bin ich lieber raus." (Proband 26)*

Die Regelmäßigkeit von Updates für Applikationen spielte insbesondere in Bezug auf die wahrgenommene Zuverlässigkeit eines Entwicklers eine Rolle. Da jede Form von Software Fehler („Bugs") und Sicherheitslücken enthalten kann, ist die Pflege der eigenen Software ein wichtiger Punkt für die Bewertung der Sicherheit der eigenen Privatsphäre. Insofern prüften Teilnehmer, wie lange das letzte Update zurückliegt.

> *„… diese hier wurde zuletzt am 20. Januar 2015 geupdated, wohingegen diese hier das letzte Update am 10. Februar 2013 bekam. Die letztere ist also klar älter und wird wohl nicht mehr gepflegt." (Proband 23)*

Insbesondere bei eher unbekannten Entwicklern wurden die weiteren, durch den gleichen Entwickler angebotenen, Dienste bzw. Applikationen betrachtet. Zum einen ob und wenn ja wie viele andere Applikationen angeboten werden und zum anderen, wie gut die se bewertet werden, ob es Beschwerden über anderen Produkte gibt und ähnliches.

> *„… wenn sie von einem unbekannten Entwickler kommt, prüfe ich im Internet, ob ich etwas über die App finden kann oder ob andere Nutzer sich über die Produkte des Entwicklers beschweren." (Proband 26)*

2.1.3.3. Sozialbasierte Heuristiken

Eine etablierte Methode zur Bewertung der Vertrauenswürdigkeit ist soziales Feedback. Wie viele Downloads hat eine App, wird die App von Freunden empfohlen, bekommt sie von Nutzern gute Reviews, wie ist die Sterne-Bewertung durch andere.

Die Anzahl der Downloads einer Applikation hing für die Teilnehmer direkt mit der Vertrauenswürdigkeit zusammen. Dies beruht auf der Annahme eines „selbstbereinigenden Prozesses" innerhalb der Applikation-Stores. Nicht vertrauenswürdige Applikationen würden zu schnell entfernt, als dass eine große Anzahl von Downloads akkumuliert werden könnte.

> *„In Bezug auf populäre Apps, die häufig heruntergeladen werden, ja, ich würde darauf vertrauen, dass es einige Menschen gibt, die bemerken würden, wenn es da Probleme mit der Privatsphäre gäbe." (Proband 21)*

Häufig werden auch Freunde oder Bekannte gefragt, insbesondere wenn eine bestimmte Funktionalität gesucht und das eigene Wissen als unzureichend wahrgenommen wird.

> *„Für mich ist hilfreich, eine Empfehlung von einem kompetenten Freund zu haben, oder es muss auch kein Freund sein, nur von einer kompetenten Person, von der ich glaube, dass sie nach ähnlichen Dingen Ausschau hält wie ich." (Proband 5)*

In den Reviews zu Applikationen suchten einige Teilnehmer auch explizit nach der Nennung von Privatsphäre-relevanten Problemen oder auch nach der Bewertung, ob die Berechtigungen angemessen und akzeptabel seien. Hierbei wurden vor allem auch die negativen Reviews geprüft. Auch Foren oder andere Online-Communities wurden als Datenquelle erwähnt. Teilweise wurden auch spezifische Webseiten genannt, die sich mit dem Vergleich von Applikationen beschäftigen, sodass der (ggf. langwierige) Vergleichsprozess ausgelagert werden kann. Auch die subjektiv größere Kompetenz der Autoren solcher Webseiten wurde genannt.

> *„Ich finde es interessant zu wissen, wenn Leute schlechte Reviews geben, ob diese auf etwas Substanziellem beruhen oder nicht." (Proband 3)*

2.1.3.4. Vermeidungsbasierte Heuristiken

Hierbei handelt es sich um Heuristiken zum Vermeiden bzw. Reduktion an Applikationen sowie von Datenflüssen. Hierunter fallen die Reduktion der Anzahl von Applikationsinstallationen an sich, die Suche nach Privatsphäre-freundlichen Alternativen sowie das Vermeiden von kostenlosen Applikationen. Darüber hinaus können besonders persönliche oder sensitive Daten an sichereren Orten als dem Smartphone, wie z.B. einer Back-Up Lösung ohne Internetanschluss, gespeichert werden. Alternativ wurde auch die Verwendung eines zweiten Gerätes (z.B. ein Altgerät) ohne weitere Daten vorgeschlagen, um nicht vertrauenswürdige Applikationen zu nutzen, sodass persönliche Daten des aktuellen Gerätes nicht in Gefahr kommen. Auch das persönliche Baugefühl fand hierbei Beachtung, „negative vibes" sollten vermieden werden.

Da viele Applikationen den Zugriff auf bestimmte, ggf. sensible oder persönliche, Informationen erfordern, ist es eine Möglichkeit die Anzahl der Installationen auf das Notwendige zu reduzieren. Auch die regelmäßige Prüfung auf nicht mehr genutzte und somit obsolete Applikationen spielte hier eine Rolle. Diese sollten dann deinstalliert werden.

> *„Ich installiere nur Apps, bei denen ich ein klares Gefühl habe, dass diese mir helfen. Ich prüfe einfach, ob ich diese App wirklich brauche." (Proband 12)*

Eine weitere Heuristik war, sich Applikationen zu suchen, die nach Möglichkeit genau das können, was benötigt wird und nicht mehr. Beschränkt sich eine Applikation in ihrer Funktionalität auf die gewünschten Features, anstatt noch für den Nutzer überflüssige zu bieten, reduziert sich häufig auch der Bedarf an Zugriffsberechtigungen. Außerdem wird durch die reduzierte Komplexität die Bewertung der geforderten Berechtigungen erleichtert.

> *„Bei diesen Riesen-Apps mit 21 Features, das kann doch keiner allein entscheiden, ob die Berechtigungen wirklich ok sind oder nicht. Ich mein, meist ist es so, dass es eine App gibt, die kann nur 3 Dinge und eines davon ist genau das, was ich brauche. Diese sind dann einfacher zu prüfen." (Proband 25)*

Bei kostenlosen Applikationen gingen unsere Teilnehmer häufiger von einer erhöhten Datensammlung aus. Wenn es eine kostenpflichtige Applikation gibt, die weniger Zugriffsberechtigungen braucht, war das für die Teilnehmer eine Gelegenheit für mehr Privatsphäre.

> *„Ich würde in jedem Fall lieber eine App kaufen, wenn sie dafür weniger Berechtigungen hat, als dass ich zu viele Berechtigungen akzeptiere." (Proband 7)*

Eine Reduktion von ggf. gefährlichen Datenflüssen erreichten verschiedene Teilnehmer beispielsweise durch den Verzicht auf das Speichern sensibler bzw. persönlicher Informationen auf dem Smartphone. So können Fotos beispielsweise entweder gar nicht auf dem Smartphone gespeichert werden oder regelmäßig auf ein anderes Gerät, wie einen Desktop PC, übertragen (und auf dem Smartphone gelöscht) werden. Auch die Verwendung eines zweiten, möglicherweise älteren, Zweitgerätes für eher invasive Applikationen wurde empfohlen.

> *„… oder noch besser, speichere keine Fotos auf dem Smartphone oder, falls möglich, übertrage sie. So kann ich sie auf meinem PC speichern, sodass sie zwar noch da sind, aber ich dennoch die App benutzen kann." (Proband 4)*

Schließlich wurde auch das Bauchgefühl, zumeist auf Basis der eigenen Erfahrung geformt, als eine Entscheidungshilfe empfohlen. Insbesondere bei der Bewertung, ob Berechtigungen angemessen sind oder ob ein spezifischer Entwickler vertrauenswürdig ist.

> *„Ja, die Datenschutzbestimmungen sind häufig verwirrend und ich lese sie dann normalerweise nicht komplett. Insofern ist es zumeist eine intuitive Entscheidung." (Proband 20)*

2.1.3.5. Zwischenfazit zur Auswahl von Smartphone Applikationen

Auf Basis der gefundenen Heuristiken ist es Experten möglich, für sie selbst zufriedenstellende Entscheidungen hinsichtlich der Installation von Applikationen zu treffen. Drei der gefundenen vier Kategorien von Heuristiken erfordern keine gesonderte Ausbildung oder Wissen (d.h. Expertenstatus), um sie anzuwenden. Diese sind die entwicklerorientierten, sozial- und vermeidungsbasierten Heuristiken. In Folge dessen soll im weiteren Verlauf insbesondere auf den vierten Typ, die berechtigungsbasierten, der Fokus gelegt werden. Hierfür wird zunächst geprüft, welche Informationen zur Umsetzung dieser dem Anwender bereits zur Verfügung stehen. Hierzu wird zunächst ein Überblick über die etablierten Berechtigungsinterfaces im mobilen Kontext gegeben. Hierbei sollen sowohl der Markführer Android (Google) als auch das größte Konkurrenzsystem iOS (Apple) beschrieben werden. Danach werden zusätzlich Empfehlungen zur Gestaltung von Berechtigungsanzeigen aus der Literatur beschrieben, um hieraus schließlich Anforderungen an ein Prototypen-Interface abzuleiten.

2.2. Überblick über Berechtigungssysteme im mobilen Kontext

Im weltweiten Markt von Smartphones sind im Augenblick zwei Systeme dominant. Das ist zum einen Android[14], welches von Google entwickelt, durch verschiedenen Hersteller für ihre Smartphones lizensiert wird und im Augenblick mit großem Abstand den größten Marktanteil hat[15], wenn die verschiedenen aktiven Version zusammengefasst werden. Zum anderen ist das iOS, welches von Apple[16] entwickelt und ausschließlich für die eigenen Mobilgeräte verwendet wird.

In Hinblick auf die Darstellung und Behandlung von Berechtigungen bei Applikationen gibt es bei Android jedoch Unterschiede, je nach verwendeter Version auf dem Endgerät. Insofern sollen im Folgenden die zwei aktuell in Verwendung befindlichen Versionen (Version 6 und neuer sowie Version

[14] www.android.com
[15] http://gs.statcounter.com/os-market-share/mobile/worldwide ; letzter Abruf 04.10.2017
[16] www.apple.com

5 und älter) sowie die ursprüngliche („legacy“) beschrieben werden. Letztere wird zwar nicht mehr aktiv verwendet, jedoch in der Literatur häufig als Referenz bzw. Vergleich herangezogen. Außerdem dient sie in Kapitel 3 als Kontrollgruppe für die Evaluation eines eigenen Berechtigungsinterfaces. Danach wird die Darstellung in iOS beschrieben und ein Fazit gezogen.

2.2.1. Android Legacy

Die ursprüngliche Darstellung der Berechtigungen in Android zeigt Abbildung 3a. In dieser Darstellung wurden im oberen Teil, zusammengefasst in verschiedene Gruppen, die potenziell gefährlichen Berechtigungen als Liste mit kurzen Erklärungen aufgeführt. Als potentiell gefährliche Berechtigungen galten hierbei jene, die durch Google als „Gefährlich“ klassifiziert wurden [17]. In Android werden Berechtigungen in drei Gruppen eingeteilt:

1. Normal – Berechtigungen, die Zugriff auf Ressourcen ermöglichen, mit welchen der Anwender gestört, aber nicht ernstlich gefährdet werden kann

2. Gefährlich – Berechtigungen, die Zugriff auf Ressourcen ermöglichen, die Kosten verursachen könnten und/oder persönliche Informationen enthalten

3. Signature/System – Berechtigungen, die Zugriff auf systemkritische Ressourcen ermöglichen; diese können nicht auf dem normalen Installationsweg angefordert werden

Durch einen Klick auf „Alle anzeigen“ konnten auch die durch Google als „Normal“ eingestuften Berechtigungen eingeblendet werden.

2.2.2. Android 5.x und älter

Im Juni 2014 führte Google ein umfangreiches Update des Play Stores durch und modifizierte hierbei auch die Darstellung der Berechtigungen einer Applikation bei der Installation. Abbildung 3A

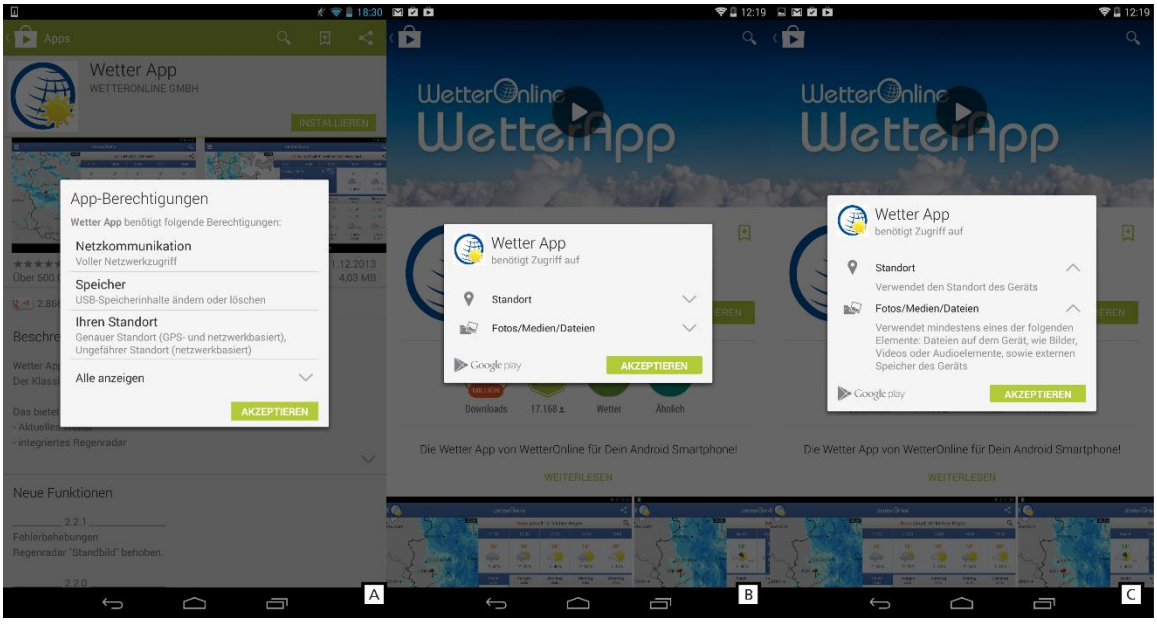

Abbildung 3. (A) Berechtigungsanzeige des Google Play Stores bis einschließlich Version 4.6.17 (B) entsprechende Darstellung seit Version 4.8.19 (C) entsprechende Darstellung mit aufgeklappten Erläuterungen

[17] https://developer.android.com/guide/topics/permissions/requesting.html#normal-dangerous ; letzter Abruf 04.10.2017

zeigt die bis dahin (Play Store Version 4.6.17) aktuelle Darstellung für die App „Wetter App“. Abbildung 3B und C die jeweils entsprechende Darstellung seit Play Store Version 4.8.19, wobei die mittlere Darstellung unmittelbar dann erscheint, wenn der Anwender auf „Installieren“ drückt. Die rechte Darstellung zeigt die gleiche Darstellung mit aufgeklappten Details. Die beiden letzteren entsprechen dem Stand, wie er für alle Android Geräte mit Version 5.x oder älter verwendet wird.

Die Berechtigungen sind hierbei in insgesamt dreizehn neue Berechtigungsgruppen unterteilt. Diese sind in der Onlinedokumentation von Google[18] aufgelistet und näher beschrieben. Sie unterscheiden sich hierbei deutlich von den Kategorien der älteren Darstellung (vgl. Kapitel 2.2.1 ab Seite 19). Wie in Abbildung 3B dargestellt, werden dem Anwender bei Drücken des Installieren-Buttons die Gruppen, zu denen die von der App angeforderten Berechtigungen gehören, inklusive des zugehörigen Symbols angezeigt. Rechts neben jeder Gruppe befindet sich ein Pfeilsymbol. Hiermit kann der Anwender eine etwas detailliertere Beschreibung zur jeweiligen Berechtigungsgruppe erhalten. Diese beinhaltet nicht die vollständige Liste der geforderten Berechtigungen der jeweiligen Gruppe, sondern eine generische Beschreibung der gesamten Gruppe. Auf diesem Wege ist keine vollständige Liste aller geforderten Berechtigungen verfügbar.

Des Weiteren werden an dieser Stelle nur die ersten zwölf der dreizehn Berechtigungsgruppen angezeigt. Die dreizehnte („Sonstiges“) findet sich nur in der gesonderten Darstellung (vgl. Abbildung 4A), in welcher sich auch die vollständige Liste der geforderten Berechtigungen findet. Das kann zur Folge haben, dass erweiterte Berechtigungen bei einer neuen Version der Applikation durch den Anwender nicht zu prüfen sind, da sie nicht angezeigt werden (vgl. Abbildung 4B und C).

Der Anwender hat bei der Installation nur die Wahl entweder allen geforderten Berechtigungen zuzustimmen oder auf die betreffende App zu verzichten. Es kommt hinzu, dass eine Zustimmung zu

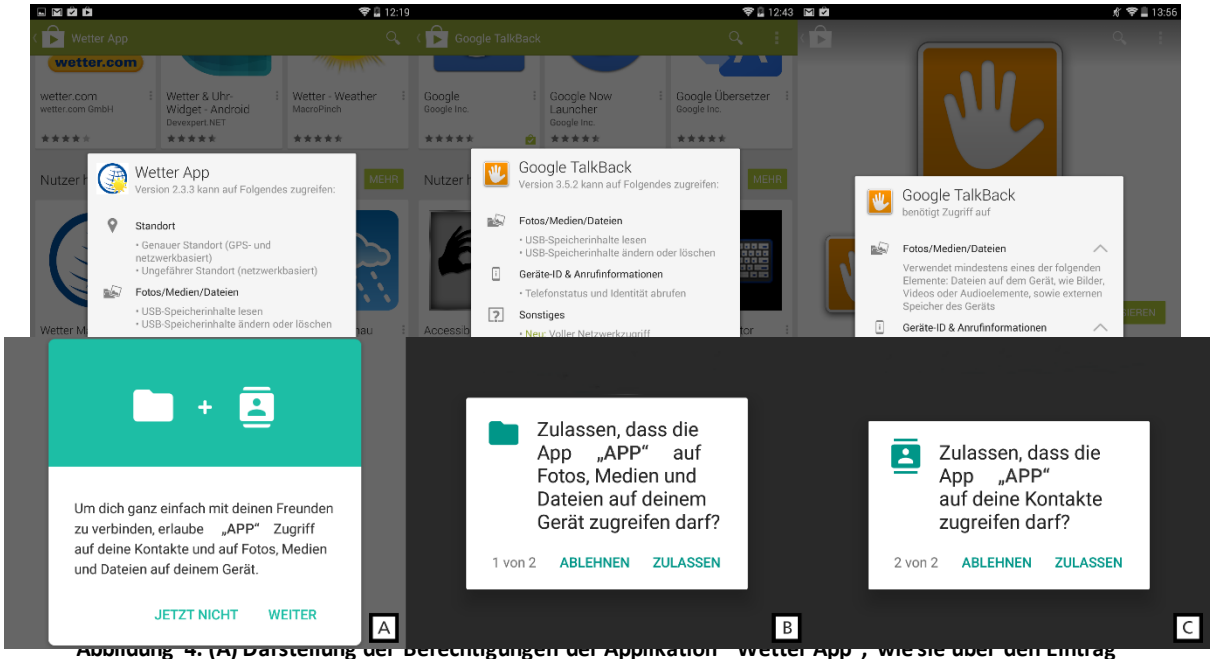

Abbildung 4: (A) Darstellung der Berechtigungen der Applikation „Wetter App“, wie sie über den Eintrag

Abbildung 5. Der Dialog zur Anfrage einer Berechtigung während der Laufzeit einer Applikation in Android 6.0 und neuer (hier Version 7.1.1), wobei (A) die optionale Begründung für die Anfrage zeigt sowie (B) und (C) die eigentliche Berechtigungsanfrage darstellen

[18] Onlinedokumentation „App-Berechtigungen prüfen“ von Google https://support.google.com/googleplay/answer/6014972?hl=dehttps://support.google.com/googleplay/answer/6014972?hl=de; letzter Abruf 04.10.2017

den geforderten Berechtigungen ebenfalls eine Zustimmung zur entsprechenden Berechtigungsgruppe beinhaltet. Dies bedeutet, dass eine App, welcher bei Installation beispielweise der lesende Zugriff auf den USB-Speicher gewährt wurde (also die Gruppe „Fotos/Medien/Dateien“) in einem zukünftigen Update, ohne weitere Benachrichtigung des Anwenders, alle weiteren Berechtigungen dieser Gruppe anfordern kann und bewilligt bekommt. Sie könnte also, ohne Wissen des Anwenders, in Zukunft auch mit der „Ändern und Löschen“-Berechtigung auf den USB-Speicher zugreifen.

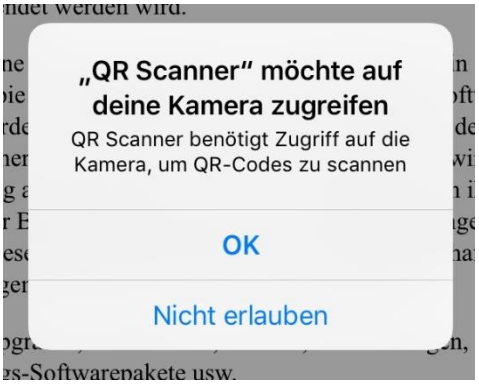

Abbildung 6. Der Dialog zur Anfrage einer Berechtigung während der Laufzeit einer Applikation in iOS (Version 10.3.3)

2.2.3. Android 6.0 und neuer

Seit Version 6.0 zeigt Android beim Betätigen des Installieren-Buttons im Play Store keine Übersicht über die Berechtigungen mehr an. Applikationen fordern Berechtigungen nun während der Laufzeit mittels Pop-Ups an, welche durch den Anwender bestätigt oder abgelehnt werden. Hierbei wird auch optional angeboten, eine Erläuterung dazu anzuzeigen, warum diese Berechtigung angefordert wird. Dies hängt jedoch vom Entwickler der Applikation ab und der Anwender hat darauf keinen Einfluss. Abbildung 5A zeigt eine solche optionale Begründung, Abbildung 5B und C die eigentlichen Anfragen. Bereits gewährte Berechtigungen werden hierbei nicht angezeigt. Werden mehrere Berechtigungen auf einmal angefordert, werden entsprechend viele Pop-Ups hintereinander angezeigt. Es können hierbei, im Gegensatz zu den früheren Android Versionen, auch einzelne Berechtigungen abgelehnt und andere zugelassen werden.

Im Play-Store selbst gibt es weiterhin die detailliertere Darstellung als Übersicht über alle ggf. während der Laufzeit angeforderten Berechtigungen, sortiert nach den dreizehn Berechtigungsgruppen, welche bereits aus Android 5.x und älteren Versionen bekannt sind (vgl. Kapitel 2.2.2 ab Seite 19).

Android bietet darüber hinaus die Möglichkeit, bereits gewährte Berechtigungen für einzelne Applikationen wieder zurückzunehmen. Diese Möglichkeit ist jedoch insofern beschränkt, dass nicht alle Berechtigungen, die es in Android gibt, individuell geregelt werden können. So wird beispielsweise der Zugriff auf die Internetverbindung jederzeit durch das System gewährt, ohne dass der Anwender dies individuell regeln könnte oder einen entsprechend Pop-Up angezeigt bekommt. Insgesamt können im Augenblick (Version 7.1.1) insgesamt dreizehn Berechtigungen geregelt werden, welche in Tabelle 1 auf der linken Seite zusammengefasst werden.

2.2.4. iOS

Apple nutzt in iOS den gleichen Ansatz, den Google auch in Android 6.0 (vgl. Kapitel 2.2.3 ab Seite 21) und neueren Versionen für die Berechtigungsvergabe nutzt. Hierbei werden Berechtigungen nicht bei der Installation angezeigt und durch den Anwender bestätigt, sondern während der Laufzeit der Applikation jeweils durch ein Pop-Up angefordert und durch den Anwender bestätigt oder abgelehnt. Abbildung 6 stellt ein solches dar.

iOS bietet hierbei, ähnlich wie auch Android, dem Entwickler die Möglichkeit, eine kurze Erläuterung, wofür die Berechtigung benötigt wird, hinzuzufügen, dies ist aber nicht verpflichtend. Die

Erläuterung wird in kleinerer Schrift direkt im Dialogfenster angezeigt (vgl. Abbildung 6). Bereits gewährte Berechtigungen werden nicht angezeigt, sodass eine Bewertung von Interaktionen zwischen Berechtigungen (z.B. Zugriff auf Kontakte & Internet) nicht möglich ist. Eine Ansicht, welche Berechtigungen generell von der Applikation angefragt werden können, existiert im App Store nicht.

Ebenfalls vergleichbar zu Android in den neueren Versionen bietet iOS die Möglichkeit, dass Anwender im Nachhinein einzelne Berechtigungen für Applikationen wieder entfernen. Auch können einzelne Berechtigungen gewährt und andere verweigert werden. Tabelle 1 zeigt eine Übersicht der in iOS (Version 10.3.3 vom 19. Juli 2017) im Reiter „Datenschutz" durch den Anwender individuell regelbaren Berechtigungen.

2.2.5. Zwischenfazit und Bewertung der Systeme

Android 6 und iOS unterscheiden sich insgesamt vergleichsweise wenig, abgesehen davon, dass iOS keine Anzeige der eventuellen Berechtigungen bereits innerhalb des App Stores bietet. Des Weiteren gibt es geringe Unterschiede bei den regelbaren Berechtigungen, z.B. SMS bei Android oder dass die Spracherkennung bei iOS gesondert vom Zugriff auf das Mikrofon regelbar ist. Großer Pluspunkt im Vergleich zu Android 5.x und älter ist bei beiden die Vermeidung des „Alles-oder-Nichts" Ansatzes, sodass auch einzelne Berechtigungen verweigert werden können, ohne auf die ganze Applikation verzichten zu müssen. Ebenfalls positiv hervorzuheben ist die Möglichkeit für den Entwickler, eine funktionale Begründung für die jeweilige Berechtigungsanfrage beizufügen. Dass diese jedoch optional bleibt und, zumindest bei Android, mit einem gesonderten Pop-Up geregelt wird erscheint nicht vollständig konsequent.

Dennoch bieten beide jedoch eine deutlich weniger granulare Regelbarkeit, als das eigentliche (d.h. technisch darunterliegende) Berechtigungssystem ermöglichen würde – d.h. es gibt deutlich mehr Berechtigungen, als für den Endanwender direkt regelbar sind. So gibt es z.B. keine Regelbarkeit des Zugriffs auf die Internetverbindung oder eine Differenzierung zwischen Lese- und Schreibzugriffen,

Tabelle 1. Übersicht über die durch den Anwender individuell regelbaren Berechtigungen in iOS bzw. Android, in der originalen Formulierung des jeweiligen Betriebssystems

Android*	iOS**
Kalender	Kalender
Kamera	Kamera
Kontakte	Kontakte
Körpersensoren	Bewegung und Fitness
Mikrofon	Mikrofon
SMS	Bluetooth-Freigabe
Speicher	Fotos
Standort	Ortungsdienste
Telefonfunktion (d.h. jemanden anrufen)	Spracherkennung
Zugriff auf Google Fotos	Homekit (d.h. Steuerung von Smarthome Geräten mittels der Apple Software Homekit)
Chatnachrichten lesen	Medien & Apple Music
Chatnachrichten verfassen	Erinnerungen
Fahrzeuginformationen	

* Version 7.1.1; ** Version 10.3.3

obwohl entsprechende Berechtigungen dennoch von jeder Applikation beim Betriebssystem angefragt werden müssen.

Eine weitere Schwäche ist, dass beide bei der Berechtigungsanfrage für den Anwender keine Möglichkeit bieten, die bereits gewährten Berechtigungen einzusehen, sodass eine Bewertung im Kontext nicht ermöglicht wird. So kann z.B. der Zugriff auf die Kamera durch eine Applikation wie einen QR-Code-Scanner als deutlich weniger bedenklich eingestuft werden, wenn kein Internetzugriff besteht. Dies ist jedoch nicht aus den Anfragen zu schließen. Die Kombination verschiedener Berechtigungen kann jedoch ein guter Indikator für schadhafte Applikationen sein [23], [24].

Ebenfalls fehlen allen neueren Ansätzen, im Gegensatz z.B. zur Android Legacy Darstellung, weiterführende Erklärungen zur jeweiligen Berechtigung. Der Anwender erfährt nicht, auf was konkret die jeweilige Applikation zugreifen kann und was das für ihn bedeuten könnte [25]. Es werden häufig für den Endanwender eher schwer verständlicher technischer Jargon [19] oder sehr unpersönliche Formulierungen [21] verwendet. So wurde z.B. die ursprüngliche Formulierung „Ihr Standort“ zu „Standort“ geändert, die einen semantischen Bezug zur Person des Anwenders vermeidet.

Insbesondere beim Wechsel von der Legacy Darstellung zur Darstellung wie sie aktuell für alle Android 5.x oder älteren Geräte verwendet wird fällt auch der Verlust von Granularität auf. Es werden nun nur noch insgesamt dreizehn Berechtigungsgruppen abgefragt (wovon eine im Interface nach dem „Installieren“-Button gar nicht angezeigt wird) und eine Bestätigung beinhaltet stets alle enthaltenen Berechtigungen [21]. Eine Applikation hat somit vollen Zugriff auf den internen Speicher, wenn die entsprechende Gruppe bestätigt wird, eine Begrenzung auf einen schlichten Lese-Zugriff ist nicht möglich, da jede neu angefragte Berechtigung aus bereits bestätigten Gruppen direkt, ohne Information für den Anwender, durch das System akzeptiert wird. Hinzu kommt, dass in einigen Fällen offenbar thematisch zusammengehörende Berechtigungen dennoch in unterschiedlichen Gruppen eingeordnet sind [21]. So enthält die Berechtigungsgruppe „Identität“ z.B. die Berechtigungen „Konten auf dem Gerät suchen“[19] und „Konten hinzufügen oder entfernen“[20]. Die Berechtigungen „Konten erstellen und Passwörter festlegen“[21] und „Konten auf dem Gerät verwenden“[22] sind jedoch unter „Sonstiges“ zu finden und somit für den Anwender bei der Installation nicht sichtbar.

Des Weiteren gibt es zwar für die Applikationen an sich Bewertungen durch Anwender, jedoch nicht für die Berechtigungen. So empfehlen die interviewten Experten die Überlegung und Bewertung, ob Berechtigungen für die jeweils gebotenen Funktionalitäten angemessen sind (vgl. das Kapitel 2.1.3.1 ab Seite 15), es gibt aber keine Möglichkeit, diese Bewertungen zu sammeln und anderen Anwendern zur Verfügung zu stellen, um diesen bei ihren Entscheidungen zu helfen.

Für alle Systeme gilt, dass es keine temporäre, zeitlich oder auch räumlich begrenzte (nur für eine Stunde, nur zu Hause o.ä.) Genehmigung gibt. Einen solchen „Geofencing“-Ansatz, die Verknüpfung der aktuellen Position mit einer bestimmten Funktion oder Aufgabe, nutzen beide Betriebssysteme bereits z.B. für die Erinnerungs- und Terminfunktionen. Eine Erweiterung auf die Gewährung von Zugriffsberechtigungen wäre somit ebenfalls denkbar, sodass eine Messenger-Applikation z.B. keinen

[19] Ermöglicht der App, eine Liste der dem Telefon bekannten Konten abzurufen. Dabei kann es sich um Konten handeln, die von installierten Apps erstellt wurden.

[20] Ermöglicht der App, Konten hinzuzufügen und zu entfernen oder deren Passwörter zu löschen.

[21] Ermöglicht der App, die Kontoauthentifizierungsfunktionen des Konto-Managers zu verwenden, einschließlich der Funktionen zum Erstellen von Konten sowie zum Abrufen und Festlegen der entsprechenden Passwörter.

[22] Ermöglicht der App, Authentifizierungs-Token anzufordern.

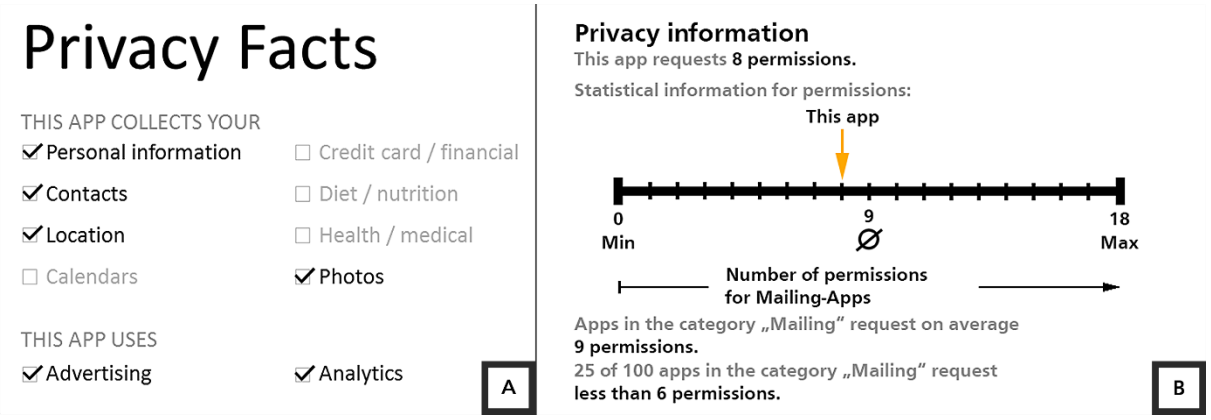

Abbildung 7. (A) Links die "Privacy facts" nach Kelley et al. (B) Rechts das Berechtigungsinterface welches Kraus et al. vorgeschlagen haben

Zugriff auf Mikrofon oder Kamera gewährt bekommt, solange man sich in sensiblen Bereichen, wie z.B. dem Arbeitsplatz oder Meetingräumen befindet.

Es zeigt sich, dass es durchaus noch Raum für Verbesserungen bei der Darstellung der Informationen, die für die Auswahl von Applikationen nach Expertenmeinung sinnvoll sind, gibt. Im folgenden Kapitel werden deshalb zunächst alternative Vorschläge für Berechtigungsdarstellungen aus der Forschungsliteratur beschrieben. Auf Basis dieser sowie der Beobachtungen aus den bisherigen beiden Kapiteln werden danach Anforderungen für einen eigenen Interface-Prototypen abgeleitet sowie ein Fazit für das weitere Vorgehen gezogen.

2.3. Überblick zu alternativen Berechtigungsdarstellungen aus der Forschung

Für die Suche nach alternativen Berechtigungsdarstellungen in der Literatur wurden zunächst die Proceedings der letzten Jahre der beiden Konferenzen CHI[23] und SOUPS[24] durchsucht. Beide stellen die zwei Top Konferenzen für „Mensch-Computer-Interaktion" in Kombination mit „Usable Security" und „Usable Privacy" dar. Darauf aufbauend wurde sowohl eine Vorwärts- wie auch Rückwärtssuche auf Basis der jeweiligen Referenzen durchgeführt. Es wurde nach Publikationen gesucht, die sich mit Zugriffsberechtigungen im Kontext von Applikationsauswahl mit dem spezifischen Fokus auf alternativen Interface Vorschläge beschäftigen. Hierbei wurden nur Publikationen berücksichtigt, die ihren Vorschlag auch in zumindest einer empirischen Studie evaluiert haben. Jede im Folgenden aufgeführte Alternative zeigte in den jeweiligen Studien signifikant bessere Ergebnisse in Relation zur Legacy Darstellung von Android in Hinblick auf die Auswahl von Applikationen mit Privatsphären-Fokus.

Kelley et al. [26] schlagen eine Darstellung mit dem Namen „Privacy facts" vor (vgl. Abbildung 7A). Hierbei werden die Berechtigungen in zwei Kategorien geclustert: Zum einen welche Art von Daten die jeweilige Applikation sammelt und zum anderen für was die Applikation diese nutzt. In der ersten Kategorie werden insgesamt acht verschiedene Stichpunkte geführt, welche jeweils mit einem Häkchen versehen werden, wenn dies auf die Applikation zutrifft. In der zweiten Kategorie werden zwei Stichpunkte mit dem selben Layout verwendet. Diese Informationen wurden für die zugehörige Studie mit automatisierten Tools direkt aus den Quelldaten der Applikationen gewonnen.

[23] www.sigchi.org/conferences
[24] www.usenix.org/conferences/soups2017 (bzw. 2016 etc. für die älteren Jahrgänge)

Kraus et al. [27] schlagen eine Visualisierung von statistischen Kennwerten bezüglich der Berechtigungsanfrage der fraglichen Applikation in Relation zu Applikationen der gleichen Kategorie vor (vgl. Abbildung 7B). Die soll den Anwender in die Lage versetzen, Applikationen jeweils im Kontext von Applikationen mit ähnlichen Funktionalitäten zu bewerten, sodass eine überdurchschnittliche Menge geforderter Berechtigungen erkannt werden kann. Hierzu nutzen Kraus et al. eine horizontale Visualisierung der Menge der geforderten Berechtigungen (markiert durch den orangenen Pfeil) in Relation zum Durchschnitt, dem Minimum sowie dem Maximum an geforderten Berechtigungen in der gleichen Kategorie. Zusätzlich bieten sie in Textform darunter noch die Anzahl der geforderten Berechtigungen des ersten Quartils (Perzentil 25).

Lin et al. [28] schlagen einen Ansatz mit Crowd-sourcing[25] vor (vgl. Abbildung 8A). Das Ziel hierbei ist Daten dazu zu sammeln, welche Berechtigungen für die fragliche Applikation erwartet werden und welche Anfragen eher überraschend sind im Kontext der gebotenen Funktionalität. Hierzu wurde ähnlich wie bei Kelley et al. [26] mittels automatisierter Tools untersucht, ob die Berechtigungen durch die Applikation für die Grundfunktionen („Core functionality"), zum Teilen oder Markieren („sharing and tagging") oder für Werbezwecke und Marktanalysen („advertising/market analysis") genutzt werden. Aus den Antworten werden dann für jede Berechtigung Statements der Art „95% der Anwender waren überrascht, dass diese App ihre aktuelle Position an Werbeanbieter sendet" formuliert und im Interface verwendet.

Harbach et al. [29] ergänzen die Anzeige der Berechtigungen durch möglichst persönliche Beispiele. So wird z.B. die Berechtigung für den Zugriff auf den Standort mit einer Kartendarstellung, auf der die tatsächliche aktuelle Position markiert ist, ergänzt oder für die Berechtigung für den Zugriff auf die Bilder wird ein zufälliges tatsächlich auf dem Smartphone gespeichertes Bild hinzugefügt. Ziel dieses Vorgehens ist es, die möglichen Konsequenzen der Bestätigung der angefragten Berechtigung besser zu visualisieren. Der Anwender soll auf diesem Wege das bestehende Risiko besser einschätzen lernen und dieses in seine Entscheidungen mit einbeziehen. Abbildung 8B stellt dieses Interface beispielhaft dar.

[25] Das bedeutet, dass Informationen mittels groß angelegter Nutzerbefragung (die „Crowd") gewonnen werden

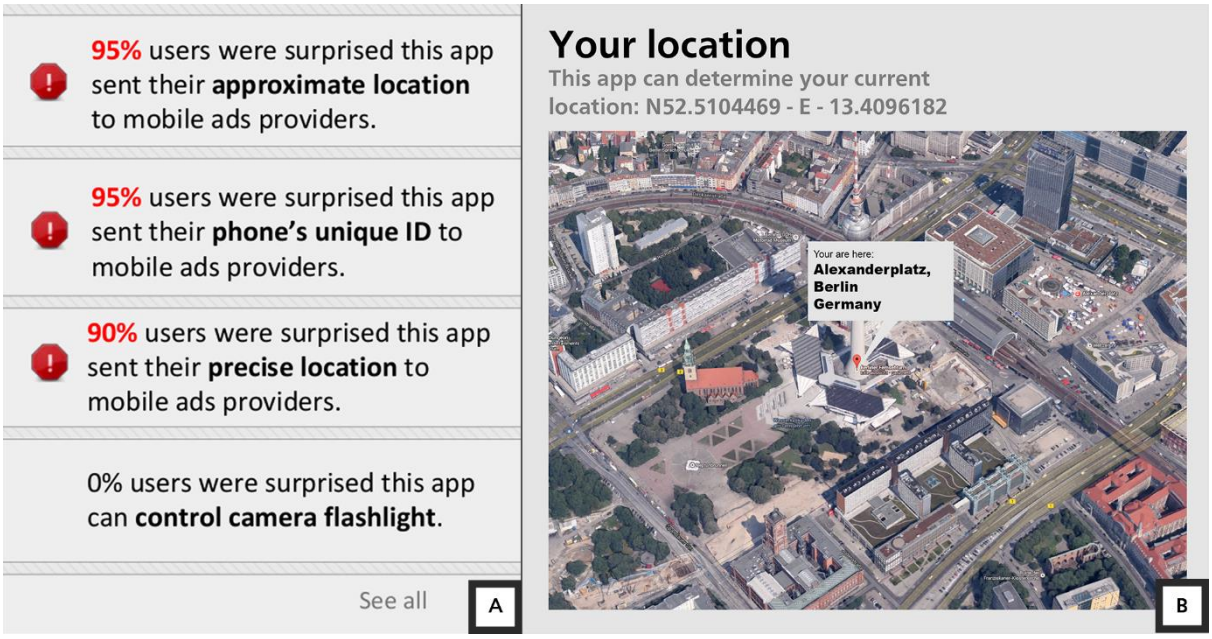

Abbildung 8. (A) Links das Berechtigungsinterface von Lin et al. (B) Rechts ein Beispiel für die Standort-Berechtigung, wie es von Harbach et al. genutzt wurde

Wang et al. [30] ergänzen die Legacy Android Darstellung in drei Vorschlägen auf der rechten Seite um Informationen über die Nutzung der jeweiligen Berechtigung durch die Applikation sowie die Option die jeweilige Berechtigung individuell abzulehnen. In der ersten Variante (Abbildung 9A) wird nur die Information ergänzt, für welche Zwecke (für die Funktionalität und/oder für Werbung) die jeweilige Berechtigung durch die Applikation genutzt wird, ohne dass eine Einflussnahme darauf hier vorgesehen ist. In der zweiten Variante (Abbildung 9B) kann die jeweilige Berechtigung individuell akzeptiert oder abgelehnt werden, ohne das die Nutzung gezeigt wird. In der dritten Variante (Abbildung 9C) können Anwender die Berechtigungen individuell ablehnen und bekommen Informationen darüber, ob die jeweilige Berechtigung für die Funktionalität, für Werbung oder für beides genutzt wird. In der letzten Variante (Abbildung 9D) schließlich kann der Anwender die Berechtigungen nicht nur individuell ablehnen bzw. akzeptieren, sondern zusätzlich die Nutzung für Werbung oder Funktionalität aktivieren bzw. deaktivieren. Damit verbunden stehen ihm naturgemäß auch die Informationen zur Nutzung der Berechtigung für Funktionalität und/oder Werbung zur

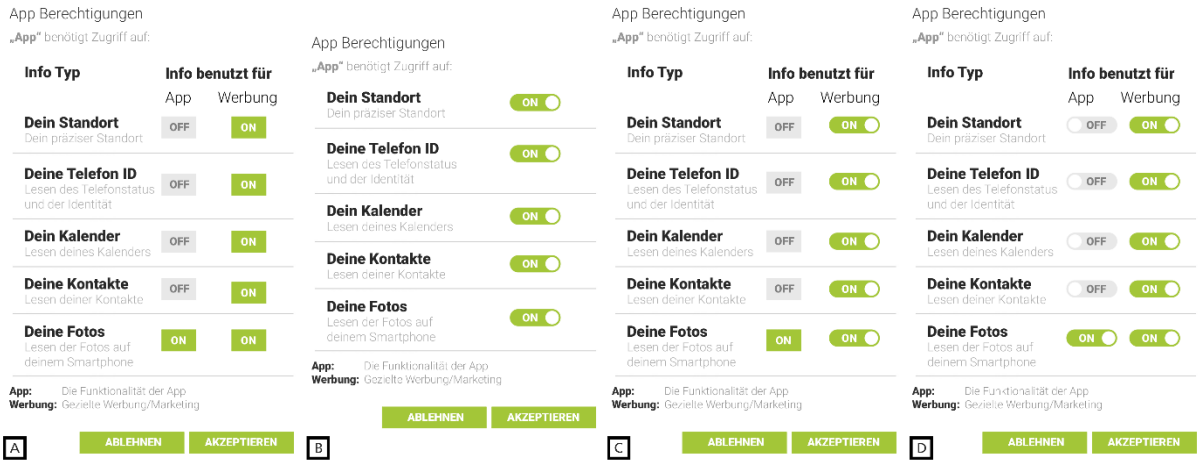

Abbildung 9. Die von Wang et al. vorgeschlagenen Varianten wobei (A) nur die Nutzungsinformationen (B) nur die Berechtigungsregelung (C) Informationen und Berechtigungsregelung und schließlich (D) Informationen und Regelung auf Funktionsniveau bietet

Verfügung. In der zugehörigen Studie konnten Wang et al. die Effektivität der Vorschläge im Vergleich zu Android Legacy Darstellung zeigen. Sowohl die Regelungsfunktionalität („Control“) als auch die Information über die Nutzung der Information („Ads awareness“) zeigen signifikante Effekte auf das Verhalten der Teilnehmer, wobei die Informationskomponente jedoch deutlich größere Effekte auf die Menge der geteilten Informationen hat ($r = -0{,}28$ vs. $r = -0{,}12$; beide jeweils hochsignifikant von 0 verschieden).

2.3.1. Ableitung von Anforderungen an eine Intervention

Zur Entwicklung einer verbesserten Darstellung, d.h. eine Intervention zur Verbesserung der Entscheidungsqualität bei der Auswahl von Applikationen für das Smartphone, werden für die weitere Arbeit die nachfolgenden Anforderungen formuliert. Diese leiten sich aus den obigen hinsichtlich der Problematik bisheriger Darstellungen sowie aus den Vorschlägen der Literatur für alternative Berechtigungsdarstellungen ab.

1. Eine Gruppierung von Berechtigungen sollte vermieden werden, d.h. dass einzelne Berechtigungen dargestellt werden sollten
2. Es sollte das gesamte Set an angeforderten Berechtigungen durch den Anwender bewertbar sein, sodass mögliche Interaktionen aus einzelnen Berechtigungen erkannt werden können
3. Die Berechtigungen sollten eine Bewertung hinsichtlich ihrer Angemessenheit für die Funktionalität haben
4. Die Berechtigungen sollten eine Bewertung in Hinblick auf ihre Gefährlichkeit, insbesondere in Kombination mit anderen Berechtigungen, haben
5. Die Darstellung sollte für den typischen Endanwender verständlich und hilfreich sein
6. Bisher bereits zur Verfügung stehende Informationen zu Downloadzahlen, Bewertungen, Reviews und grundlegenden, applikationsspezifischen Informationen sollten erhalten bleiben

Auf eine direkte Regelungsmechanik, wie Wang et al. sie vorschlagen, wird an dieser Stelle verzichtet, da diese zum Zeitpunkt der Entwicklung noch nicht im System implementiert war und in den aktuellen Versionen von Android und iOS Berechtigungen während der Laufzeit angefragt werden, nicht bei der Installation und sie somit redundant wäre. Der Ansatz von Android 6.0 bzw. iOS lässt sich dennoch mit dem im folgenden Kapitel beschriebenen und evaluierten Prototypen nutzen, wenn der aktuelle Pop-Up Dialog um die entsprechenden Informationen über bereits gewährte Berechtigungen erweitert würde. Der Regelungsmechanismus von Wang et al. wäre dann bereits implementiert.

2.3.2. Zusammenfassung und Fazit für das weitere Vorgehen

Im aktuellen Kapitel wurden auf Basis einer empirischen Befragung von insgesamt 26 IT Experten zunächst Heuristiken identifiziert, mit denen Endanwender ihre Auswahl von Applikationen für das Smartphone in Hinblick auf den Schutz der eigenen Privatsphäre verbessern können. Insbesondere kann bei Anwendung der Heuristiken bei der Installation das bewusste Auseinandersetzen mit den zur Verfügung stehenden Informationen gefördert werden. Erst auf diese Weise ist es möglich diese auch bei der Entscheidungsfindung zu berücksichtigen.

Im weiteren Verlauf wurden die verschiedenen Darstellungen von Berechtigungen in den beiden am weitesten verbreiteten mobilen Betriebssystemen Android und iOS betrachtet und analysiert. Dies folgte aus der Beobachtung, dass vor allem für die Bewertung dieser Informationen Expertenwissen hilfreich ist, wohingegen die Bewertung von Beschreibungen oder Entwicklerwebseiten auch dem

typischen Endanwender möglich ist. Insofern steht zu erwarten, dass bei der Darstellung von Berechtigungen das größte Potential zur Entscheidungsverbesserung vorhanden ist. Anders ausgedrückt liegt dort die größte Gefahr von Überforderung oder Missverständnissen auf Seiten des Endanwenders. Diese Vermutung kann durch die Literatur klar gestützt werden (z.B. [18], [19], [25], [31]).

Im Folgenden werden dann auf Basis einer Literatursuche verschiedene alternative Darstellungen betrachtet, welche sich bereits in empirischen Studien als vielversprechend erwiesen haben, um schließlich auf Basis dieser Erkenntnisse Anforderungen für die Entwicklung einer eigenen Alternative abzuleiten.

Im folgenden Kapitel wird zunächst der entwickelte Prototyp für eine Berechtigungsdarstellung beschrieben. Danach wird im Detail die zugehörige Evaluationsstudie dargestellt, welche den Prototypen sowohl mit bereits implementierten Darstellungen als auch mit Vorschlägen aus der Forschung vergleicht.

3. Evaluation eines prototypischen Berechtigungsinterfaces

Basierend auf den Anforderungen, die in den Vorarbeiten definiert wurden (vgl. Kapitel 2.3.1 ab Seite 27) wurde eine eigene Berechtigungsdarstellung entwickelt und evaluiert. Das übergeordnete Ziel hierbei war es, dass der Anwender durch bessere Information in die Lage versetzen wird, bessere Entscheidungen zu treffen. Im Kontext der Evaluationsstudie bezog sich dies auf Privatsphäre-freundlichere Entscheidungen, da dies der Faktor war, der variiert wurde, um so die Effektivität der neuen Darstellung zu testen.

Im digitalen Alltag bedeutet dies aber, dass der Anwender durch die verbesserte Darstellung in die Lage versetzt wird diese Informationen zusätzlich, d.h. neben den anderen zur Verfügung stehenden wie z.B. die Herkunft des Entwicklers oder die eigenen Präferenzen hinsichtlich der Gestaltung der Applikation, in seine Entscheidung mit einzubeziehen. Auf diese Weise sollen Entscheidungen ermöglicht werden, die möglichst gut zu den persönlichen Wünschen des Anwenders passen. Das kann, muss aber nicht die in Hinblick auf die eigene Privatsphäre beste Entscheidung sein.

Insofern werden für das aktuelle Kapitel folgende Ziele formuliert:

1. Umsetzung der im vorherigen Kapitel formulierten Anforderungen in Form einer prototypischen Darstellung von Berechtigungen
2. Design einer Evaluationsstudie zum Vergleich des Prototypens sowohl mit aktuellen als auch forschungsbasierten alternativen Darstellungen
3. Einordnung der Ergebnisse in den Forschungskontext und Ableitung von Implikationen für das weitere Vorgehen

Im weiteren Verlauf dieses Kapitels wird zunächst der gestaltete Prototyp „COPING“ vorgestellt. Im Anschluss daran wird zunächst auf die Methodik und das Design der Evaluationsstudie eingegangen, um danach die Ergebnisse darzustellen und zu diskutieren. Das Kapitel schließt mit einem zusammenfassenden Fazit und einem Ausblick auf die nächsten Arbeitsschritte.

3.1. Der Prototyp COPING

Die COPING (kurz für **CO**mprehensive **P**erm**I**ssio**N** **G**ranting) Berechtigungsdarstellung folgt den im vorherigen Kapitel definierten Anforderungen. Abbildung 10 zeigt zwei Beispiele für die Darstellung für verschiedene QR-Code-Scanner Applikationen, wie sie auch in der zugehörigen Studie verwendet wurden. Die Grundform basiert auf dem Vorschlag von Lin et al. [28], welcher bereits weiter oben beschrieben wurde (vgl. Kapitel 2.2 ab Seite 24), da dieser einen Teil der Anforderungen bereits erfüllt. Im Detail listet er bereits alle Berechtigungen einzeln auf, ohne diese zu gruppieren und fügt jeder

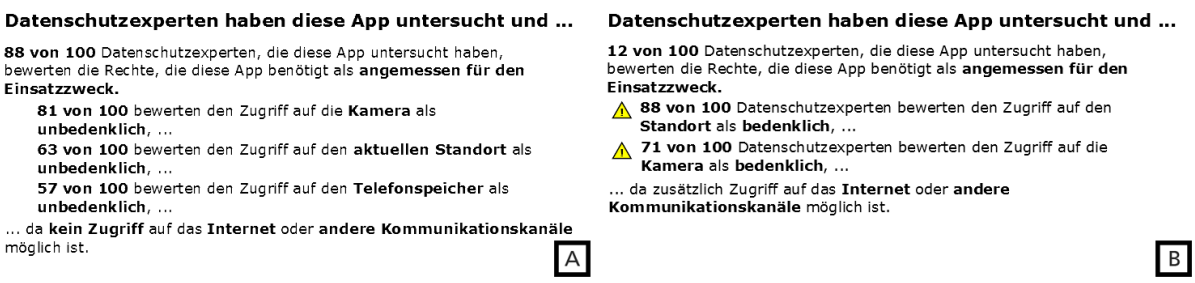

Abbildung 10. Zwei Beispiele für die Darstellung des COPING Berechtigungsprototypens für eine QR-Code-Scanner Applikation, wie sie auch in der Evaluationsstudie verwendet wurde

Berechtigung eine Bewertung hinsichtlich ihrer Angemessenheit hinzu. Dies erfüllt die erste sowie die dritte der sechs in dieser Arbeit definierten Anforderungen. Mit entsprechendem Vorwissen des Anwenders könnte auch die zweite Anforderung, die Bewertung möglicher Interaktionen zwischen einzelnen Berechtigungen, als erfüllt gelten. Da der typische Anwender aber eher nicht über Expertenwissen in Hinblick auf Berechtigungen verfügt [19], ist davon auszugehen, dass hierfür noch weitere Hilfestellung benötigt wird.

Um eine Abgrenzung von den bereits bekannten Nutzerbewertungen der Applikation zu erreichen wurde deshalb zunächst der Begriff „Anwender" gegen „Datenschutzexperten" ausgetauscht. Darauf aufbauend beginnt die Darstellung mit einer Einschätzung über die Angemessenheit der durch die Applikation geforderten Berechtigung im Hinblick auf ihre Funktionalität bzw. ihren Einsatzzweck. Dies soll die in der dritten Anforderung definierte Bewertung für den Anwender erleichtern, da er so nicht jede einzelne Bewertung der Berechtigung lesen und kombinieren muss.

Danach folgt eine Liste der Berechtigungen, die aus Expertensicht im Kontext der Funktionalität bedenklich erscheinen. Die Liste ist geordnet nach dem prozentualen Anteil der Experten, die diese Einschätzung teilen. Sie ist weiterhin gruppiert nach der jeweiligen Begründung, warum diese Einschätzung getroffen wurde. So ist im Beispiel A (siehe Abbildung 10A) der Zugriff auf die Kamera, den Standort sowie den Telefonspeicher aus Expertensicht eher unbedenklich, da die Applikation keinen Zugriff auf das Internet oder andere Kommunikationskanäle des Smartphones hat. Im Beispiel B hingegen bewerten die Experten ähnliche Berechtigungen als bedenklich, da durch den Zugriff auf die Internetverbindung die so gewonnenen Daten direkt weitergeleitet werden können und es für die Funktionalität der Applikation nicht notwendig ist. Auf diese Weise wird dem Anwender ermöglicht, auch Interaktionen von Berechtigungen in seine Entscheidung für oder gegen eine Applikation einzubeziehen.

In Hinblick auf die Kommunikation der prozentualen Anteile wurde bei COPING darauf verzichtet direkt mit Prozentzahlen zu arbeiten. Den Empfehlungen von Gigerenzer und Hoffrage [32] folgend wurden hierfür Zahlen mit natürlichem Sampling verwendet, da diese leichter zu interpretieren, wenn auch inhaltlich äquivalent, sind. Statt 88% wird also die Formulierung 88 von 100 verwendet.

Direkt von Lin et al. [28] wurde auch die Verwendung eines Warnzeichens übernommen. Dieses erscheint vor Berechtigungen, bei der mehr als die Hälfte (also 50 von 100 oder mehr) der Experten die jeweilige Berechtigung als bedenklich einstuft. Jedoch wurde das Farbschema auf Gelb/Schwarz geändert, wie es von internationalen Standards für Warnzeichen vorgesehen wird. Rot, wie bei Lin et al. verwendet, bezeichnet Verbots- oder Brandschutzzeichen [33].

3.2. Evaluation des Prototypens

Der Prototyp wurde im Rahmen einer Onlinestudie mit einem „Mix-Model Design" evaluiert. Insgesamt wurden sechs verschiedene Berechtigungsdarstellungen verglichen, wobei jedem Teilnehmer eine davon zufällig zugeteilt wurde. Jeder Teilnehmer musste daraufhin dreimal aus jeweils drei Applikationen diejenige aussuchen, die ihm am besten erschien. Alle verwendeten Darstellungen wurden mit der Legacy Android Darstellung, welche als Kontrollgruppe fungierte, verglichen. Diese wurde gewählt, da auch alle anderen verwendeten aus der Forschungsliteratur entnommenen Darstellungen mit der Legacy Darstellung verglichen wurden. Eine detaillierte Beschreibung der Studie findet sich in [22]. Alle verwendeten Versuchsmaterialien finden sich im Anhang A2 ab Seite 86.

Die Studie selbst orientiert sich am Berechtigungsparadigma, welches Android 5.x und ältere Versionen verwenden. Das bedeutet, dass die Teilnehmer alle Informationen zu den fraglichen Applikationen inklusive der Berechtigungen (die jeweils mit einer zufällig ausgefällten Darstellung abgebildet werden) als Ganzes vor ihrer Entscheidung dargestellt bekommen. Der einzige Unterschied zu Android 5.x bestand in der Verlegung der jeweiligen Berechtigungsdarstellung vom Zeitpunkt nach Betätigen des „Installieren"-Buttons in die eigentliche Applikations-Detailseite. Dieses Vorgehen ist analog zum Versuchsdesign welches Kelley et al. [26] verwendeten, welche dieses selbst von Good et al. [34] adaptierten.

Auf den Ansatz von Android 6.0 oder iOS wurde verzichtet, da diese naturgemäß eine vorherige Installation und Nutzung der fraglichen Applikationen erforderlich machen würde, da Berechtigungen nur während der Laufzeit angefragt werden. Dies würde ein gänzlich anderes Versuchsparadigma erfordern, sodass sich hier für die größere Reichweite einer Onlinestudie (in Relation zu einer Laborstudie) und bessere Vergleichbarkeit mit bisherigen Studien entschieden wurde.

Darüber hinaus sind selbst aktuell, zweieinhalb Jahre nach Planung und Durchführung der Studie sowie fast zwei Jahre nach Veröffentlichung von Android 6, noch über 50% aller aktiven Android Geräte mit Versionen älter als 6.0 ausgestattet[26]. Die Updatezyklen im Android Ökosystem sind erfahrungsgemäß sehr lang, da viele Geräte, insbesondere die günstigeren von den jeweiligen Herstellern gar keine „Major-Updates", d.h. Updates von z.B. Android 4.x auf Android 5.x, erhalten.

Blickt man über den mobilen Markt hinaus auf andere Systeme, die ebenfalls Berechtigungen für die Zugriffsregelung nutzen, zeigt sich, dass der „Bei Installation" (bzw. „vor erstem Start") Ansatz auch dort weit verbreitet ist. Exemplarisch seien hier z.B. das Management eines Google-Kontos (vgl. Abbildung 11A), die Datenschutzeinstellungen von Windows 10 (vgl. Abbildung 11B) sowie Facebook Applikationen genannt (vgl. Abbildung 11C).

Ebenso verfügen auch die Ansätze von Android 6.0 bzw. iOS über Schwächen hinsichtlich ihrer Darstellungen, wie bereits zuvor diskutiert (vgl. Kapitel 2.2 ab Seite 18). Es bleibt festzuhalten, dass die hier vorgestellten Ergebnisse trotz des Wechsels hinsichtlich des Berechtigungsmanagements beim Wechsel von Android 5.x auf Android 6.0 nicht ihre Gültigkeit bzw. Relevanz verlieren, da sie nicht einzig in diesem Kontext anwendbar sind.

Im weiteren Verlauf des Kapitels wird im Detail auf die verglichenen Berechtigungs-Darstellungen, den Studienablauf sowie die verwendeten Hypothesen, die gewählten Applikationen bzw.

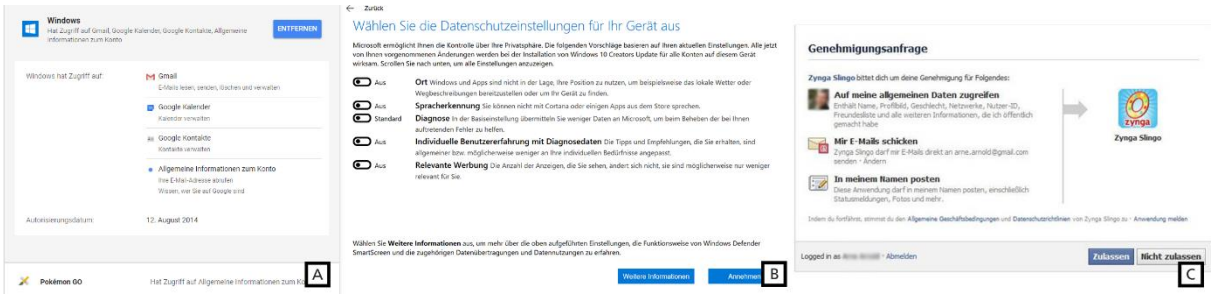

Abbildung 11. Beispiele für weitere Berechtigungsysteme nach dem Bestätigungsprinzip "Bei Installation" bzw. "Vor dem ersten Start" analog zu Android 5.x oder älter wobei (A) das Management von mit einem Googlekonto verbundenen Geräten (B) die Datenschutzeinstellungen von Windows 10 vor der Installation des Windows Creation Updates und (C) die Anfrage für Zugriffsberechtigungen einer Facebook Applikation darstellen

[26] https://developer.android.com/about/dashboards/index.html - Letzter Zugriff 13.07.2017

Entscheidungssituationen und anschließend die erhobene Stichprobe eingegangen. Danach folgt die Darstellung und Diskussion der Evaluationsergebnisse sowie ein Fazit.

3.2.1. Die verglichenen Berechtigungsdarstellungen

Eine vollständige Übersicht über die verwendeten Darstellungsvarianten inklusive einer Beschreibung der Kernkomponenten ist in Abbildung 12 zusammengefasst. Von den im vorherigen Kapitel (vgl. Kapitel 2.2 ab Seite 24) vorgestellten alternativen Berechtigungsdarstellungen aus der Forschung wurde das von Harbach et al. [29] sowie das von Wang et al. [30] nicht in der Studie berücksichtigt. Letzteres, da es zum Zeitpunkt der Studie noch nicht publiziert und somit nicht bekannt war. Ersteres aus zwei verschiedenen Gründen. Zum einen ist der Grundgedanke des Vorschlags von Harbach et al., dass dem Anwender das Risiko der Datenfreigabe dadurch vor Augen geführt wird, dass ihm persönliche Beispiele vom eigenen Smartphone angezeigt werden. Dies ist im Kontext einer Studie, ob im Labor oder Online, ohne Zugriff auf die eigentlich privaten Daten der Teilnehmer nicht möglich. Zum anderen sind die angezeigten Informationen tangential zu den Informationen aus allen anderen Darstellungsansätzen, sodass nichts dagegenspräche, die Idee von Harbach et al. mit dem besten der anderen Darstellungstypen zu kombinieren.

An den restlichen Darstellungen wurden ebenfalls einige Änderungen vorgenommen, da die Grundannahme ist, dass die Applikationen hier auf Basis der Berechtigungen beurteilt werden. Somit scheiden Informationen aus, die eine tiefgehende Code-Analyse einer Applikation erfordern würden. Dem folgend wurden die Darstellungen von Lin et al. [28] sowie Kelley et al. [26] dergestalt angepasst ohne deren Grundidee zu verlieren.

Bei den „Privacy facts“ nach Kelley wurden jene Informationen aus dem Bereich des „Sammelns“ entfernt, die nicht durch die Analyse der Berechtigungen oder anderer Meta-Informationen, welche über eine Applikation in einem App Store verfügbar wären, erschlossen werden können. Darunter fallen die Kreditkarten, Ernährungs- und Gesundheitsinformationen. Das gleiche gilt für „Werbung“ bzw. „Analyse“ aus dem Bereich der „Nutzung“. Zu beachten ist hier, dass Kelley et al. bereits dokumentierte, dass der Begriff „Analyse“ von den Teilnehmern als kaum bis gar nicht verständlich empfunden wurde. Um die Grundidee der Darstellung von Daten sammeln und nutzen zu erhalten, wurde neben dem Bereich „Die Applikation hat Zugriff auf“ der Bereich „Gesammelte Daten können durch die Applikation versendet werden über“ eingefügt. Hier sind die verschiedenen Informationskanäle, die dem Smartphone zur Verfügung stehen gelistet. Hierunter fallen z.B. Bluetooth oder WLan.

Bei Lin et al. wurde analog vorgegangen, d.h. Informationen die nicht über die Analyse der Berechtigungen oder anderer Meta-Daten verfügbar sind wurden gestrichen. Das resultierte in dem Entfernen der Begründungsstatements, welche entweder für die Grundfunktionen („Core functionality“), zum Teilen oder Markieren („sharing and tagging“) oder für Werbezwecke und Marktanalysen („advertising/market analysis“) waren.

Die Darstellung von Kraus et al. [27] wurde unverändert übernommen. Das gleiche gilt für die Legacy Darstellung von Android (Kontrollgruppe) sowie die aktuelle Darstellung für alle Versionen bis Android 5.x. Alle Berechtigungsdarstellungen wurden für die Entscheidung der Teilnehmer in eine Adaption des Google Play Store integriert, welche die restlichen Meta-Informationen, wie Downloadzahlen oder Anwenderbewertungen zur Verfügung stellte.

Die untersuchten Berechtigungsdarstellungen unterscheiden sich hierbei nicht nur in Hinblick auf ihr Layout, sondern auch in Hinblick auf den Umfang der gebotenen Informationen. Während die Legacy Android Darstellung eine lineare Liste aller Berechtigungen bietet, bieten die verschiedenen Darstellungen, verglichen damit, jeweils mehr oder weniger umfangreiche Informationen. Entsprechend lässt sich ein Ranking aufstellen, welches im späteren Verlauf die Interpretation der Ergebnisse unterstützt.

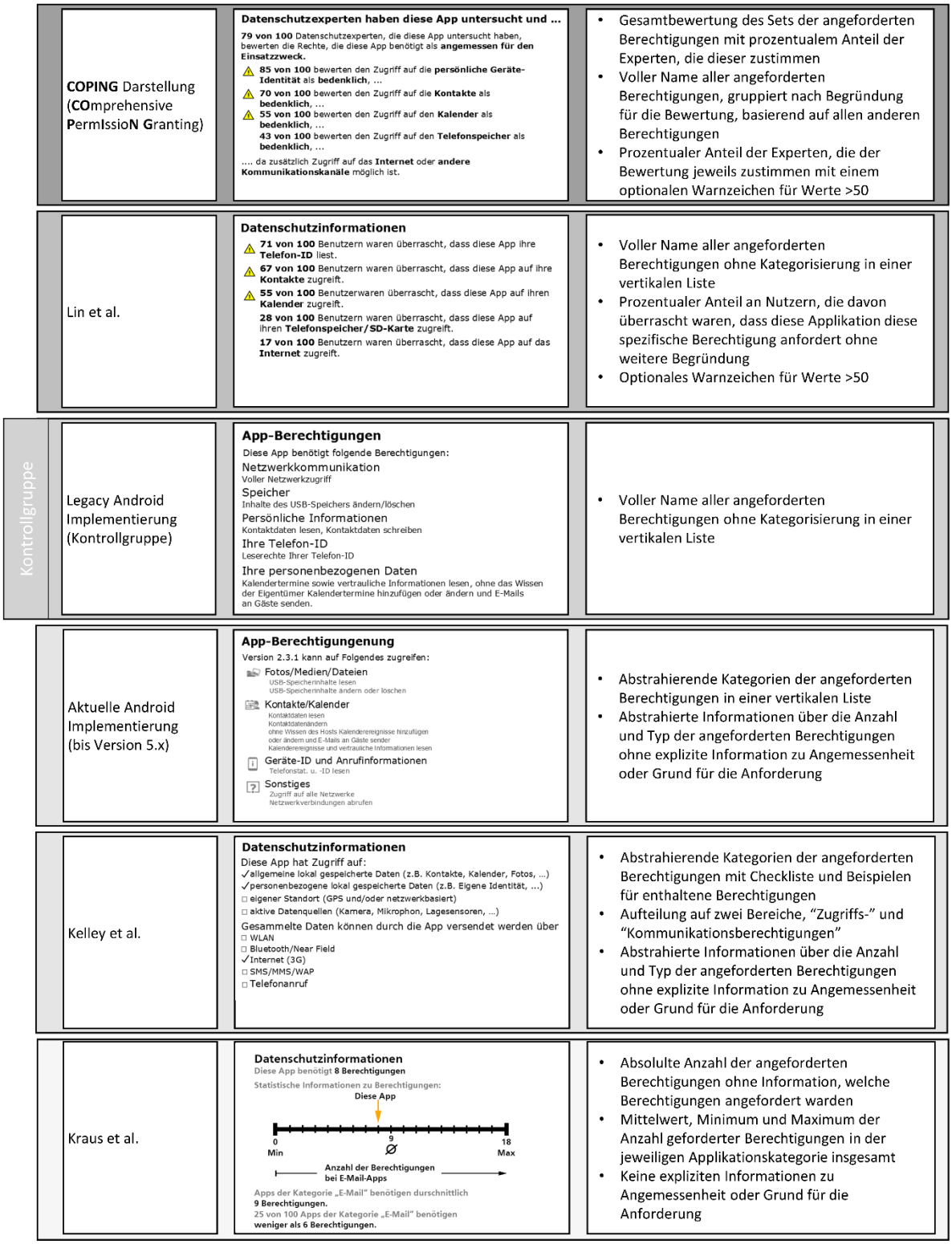

Abbildung 12. Übersicht über alle in der Evaluationsstudie verwendeten Berechtigungsdarstellungen inklusive Beispiel und Kurzbeschreibung des Aufbaus

Verglichen mit der Legacy Darstellung bieten die Vorschläge von Kraus et al., Kelley et al. sowie die Darstellung von Android 5.x weniger umfangreiche Informationen, da keine der genannten noch die einzelnen Berechtigungen, sondern stets eine gruppierte und abstraktere Darstellung bietet. Der Vorschlag von Lin et al. sowie der COPING Prototyp bieten umfangreichere Informationen verglichen mit der Legacy Darstellung, da beide zusätzlich zu der vollständigen Liste aller Berechtigungen noch weitere Informationen zur Bewertung dieser liefern. Die COPING Darstellung bietet darüber hinaus noch weitere Informationen zur einfacheren Bewertung möglicher Interaktionen zwischen den Berechtigungen, kann also als noch umfangreicher als der Vorschlag von Lin et al. bezeichnet werden. Entsprechend sind auch die Darstellungen in Abbildung 12 sortiert.

3.2.2. Studienablauf

Die Studie gliedert sich insgesamt in sieben Phasen und wurde bei SoSciSurvey[27] in Deutschland gehostet.

Phase 0: Begrüßung und Einführung. Die Studie startete mit einer kurzen Beschreibung unserer Forschungsgruppe, den vorgeblichen Zielen der aktuellen Studie, der voraussichtlichen Dauer sowie datenschutzrechtliche Informationen zur Anonymisierung der Daten sowie der Speicherdauer und dem Verwendungszweck für ausschließlich wissenschaftliche Zwecke. Das angegebene Ziel der Studie war die Erforschung der Nutzerinteraktion mit Smartphones, im Speziellen bei der Applikationsauswahl. Weder Privatsphäre noch IT-Sicherheit wurden an dieser Stelle genannt, um Priming-Effekte zu vermeiden. Die Teilnehmer wurden aufgefordert sich vorzustellen, sie hätten soeben ein neues Smartphone bekommen und würden nun einige neue Applikationen im Google Play Store suchen. Der eigentliche Zweck der Studie wurde nach Phase 3 genannt. Außerdem gab es einen Hinweis auf die Verlosung von Amazon-Gutscheinen unter allen Teilnehmern am Ende der Studie. Die dabei notwendigerweise erhobenen E-Mailadressen wurden in einer gesonderten Datenbank, getrennt von den Antworten gespeichert. Eine Verknüpfung der Daten miteinander war nicht möglich.

Phase 1: Android Erfahrung. Die Teilnehmer wurden hier gefragt, ob sie über ein Android-Mobilgerät verfügen und, falls ja, wie lange sie Android im Allgemeinen bereits verwenden. Basierend auf der Antwort erhielten die Teilnehmer eine längere oder kürzere Instruktion, bevor die eigentlichen Entscheidungssituationen bearbeitet wurden. Im Falle, dass ein Teilnehmer über kein Android-Gerät verfügte wurde der Google Play Store kurz vorgestellt, da die genutzte Darstellung in der Studie an dessen Layout orientiert war.

Phase 2: Entscheidungssituationen. Alle Teilnehmer bearbeiteten drei Entscheidungssituationen in zufälliger Reihenfolge. In jeder musste jeweils eine von drei Applikationen gewählt werden. In Abbildung 13 ist ein Beispiel für eine solche Entscheidungssituation dargestellt. Die drei Kategorien waren Sudoku, E-Mail sowie QR-Code-Scanner Applikationen. Eine detaillierte Beschreibung der drei Entscheidungssituationen findet sich im Kapitel Entscheidungssituation und gewählte Applikationen ab Seite 36.

Während der Typ der genutzten Berechtigungsdarstellung für jeden Probanden zufällig ausgewählt wurde und für alle drei Entscheidungen gleich blieb wurde das restliche Interface für die jeweiligen Entscheidungssituationen für jeden Probanden und jede Entscheidungssituation zufällig zusammengestellt. Das bedeutet, dass die Kombinationen aus Applikationsname und Beschreibung

[27] www.soscisurvey.de

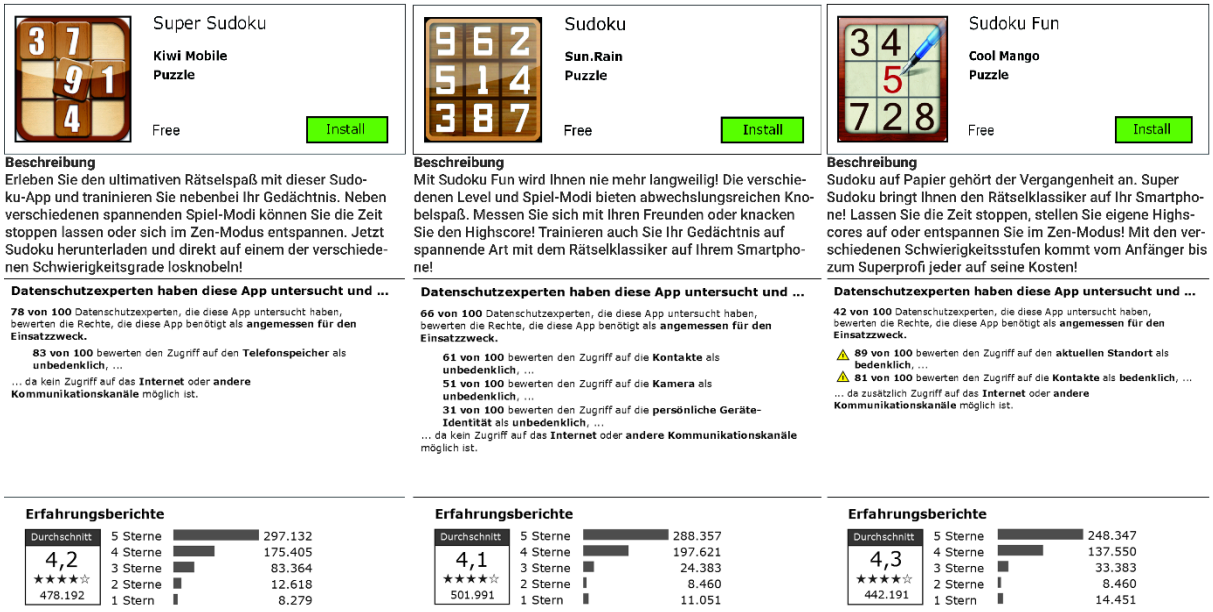

Abbildung 13. Beispiel für eine Entscheidungssituation über eine Sudoku Applikation in der Evaluationsstudie

jeweils zufällig einem Logo, einem Entwicklernamen, einer Anwender-Bewertung (Sterne-Bewertung) sowie einer Ausprägung der Berechtigungen (gut / mittel / schlecht) zugewiesen wurde. Zusätzlich wurde auch die Positionierung (links / mittig / rechts) zufällig gewählt. Um mögliche Seiteneffekte zu vermeiden, wurden die Applikationsbeschreibungen so gewählt, dass sie inhaltlich die gleichen Funktionalitäten beschreiben. Auch die Anwender-Bewertungen variierten nur zwischen 4,1 und 4,3 und die Anzahl der Bewertungen war jeweils in einer vergleichbaren Größenordnung fixiert. In dieser Phase wurde neben den eigentlichen drei Entscheidungen auch die benötigte Entscheidungszeit mit dokumentiert.

Phase 3: Fragen zum typischen Applikationsauswahlverhalten. Die Teilnehmer wurden gefragt, ob sie eine oder mehrere der Applikationen bereits kannten. Zusätzlich sollten sie schätzen, wie oft sie den Google Play Store (oder eine vergleichbare Anwendung, falls sie kein Android-Gerät besitzen) nutzen, wie viele Applikationen sie etwa auf ihrem Gerät installiert haben und wie viele verschiedene Applikationen sie etwa pro Woche nutzen. Sie wurden auch gefragt, ob ihnen Unterschiede zum normalen Aussehen des Play Stores aufgefallen sind, um zu prüfen, ob das Hinzufügen der Berechtigungsdarstellungen den Teilnehmer bewusst aufgefallen ist.

Phase 4: Fragen zur in der Studie genutzten Berechtigungsdarstellung. Mit Abschluss der dritten Phase erhielten die Teilnehmer eine kurze Erläuterung, die den eigentlich Zweck der Studie, die Untersuchung der Berechtigungsdarstellung, enthüllte. Zusätzlich wurde erneut ein Bild einer der bereits bearbeiteten Entscheidungssituationen aus Phase 2 gezeigt in dem die Berechtigungsdarstellung farblich hervorgehoben war. Sie wurden gefragt, ob sie die Inhalte der Darstellung gelesen haben, ob sie die Informationen für die Wahl der Applikation genutzt haben sowie ob sie diese Informationen als verständlich und hilfreich empfunden haben. Außerdem sollten sie einschätzen, ob eine solche Darstellung ihnen helfen würde ihre Privatsphäre besser zu schützen.

Phase 5: Allgemeine demographische Fragen. Um auch auf demographische Effekte prüfen zu können, wurden die Teilnehmer in der vorletzten Phase gebeten, einige allgemeine Informationen über ihre Person zur Verfügung zu stellen. Konkrete wurde nach dem Alter, dem Geschlecht, dem aktuellen Beruf sowie dem höchsten erreichten Schulabschluss bzw. Ausbildungsabschluss gefragt.

Phase 6: Verabschiedung und Aufklärung. Zum Abschluss gab es die Möglichkeit, sich für die Verlosung anzumelden sowie anzugeben, dass man nähere Informationen zu den Studienergebnissen erhalten möchte. Zusätzlich gab es einen kurzen Informationstext zu Berechtigungen sowie den neusten Änderungen bei Android zu diesem Thema und den damit verbundenen Risiken für den Anwender.

3.2.3. Hypothesen

Im Rahmen der Evaluationsstudie sollten, basierend auf den Erkenntnissen aus der oben dargestellten Literatur, folgende Hypothesen geprüft werden:

H1. Die Teilnehmer zeigen unterschiedliche Leistung hinsichtlich der Entscheidungsqualität[28] bei der Applikationsauswahl basierend auf der ihnen zugewiesenen Berechtigungsdarstellung.
- H1.1. Teilnehmer, die die Darstellung von Kraus et al. benutzen, zeigen eine bessere Leistung als Teilnehmer mit der Legacy Darstellung.
- H1.2. Teilnehmer, die die Darstellung von Kelley et al. benutzen, zeigen eine bessere Leistung als Teilnehmer mit der Legacy Darstellung.
- H1.3. Teilnehmer, die die Darstellung von Lin et al. benutzen, zeigen eine bessere Leistung als Teilnehmer mit der Legacy Darstellung.
- H1.4. Teilnehmer, die die COPING Darstellung benutzen, zeigen eine bessere Leistung als Teilnehmer mit der Legacy Darstellung.
- H1.5. Teilnehmer, die die Darstellung von Android 5.x benutzen, zeigen eine bessere Leistung als Teilnehmer mit der Legacy Darstellung.

H2. Die Bewertung der Teilnehmer, als wie hilfreich eine Darstellung empfunden wird, fällt unterschiedlich aus, basierend auf der ihnen zugewiesenen Berechtigungsdarstellung.

H3. Die Teilnehmer benötigen für die Auswahl einer Alternative unterschiedlich viel Zeit basierend auf der ihnen zugewiesenen Berechtigungsdarstellung.
- H3.1. Teilnehmer, die die Darstellung von Kraus et al. benutzen, treffen ihre Entscheidung schneller als Teilnehmer mit der Legacy Darstellung.
- H3.2. Teilnehmer, die die Darstellung von Kelley et al. benutzen, treffen ihre Entscheidung schneller als Teilnehmer mit der Legacy Darstellung.
- H3.3. Teilnehmer, die die Darstellung von Lin et al. benutzen, treffen ihre Entscheidung schneller als Teilnehmer mit der Legacy Darstellung.
- H3.4. Teilnehmer, die die COPING Darstellung benutzen, treffen ihre Entscheidung schneller als Teilnehmer mit der Legacy Darstellung.
- H3.5. Teilnehmer, die die Darstellung von Android 5.x benutzen, treffen ihre Entscheidung schneller als Teilnehmer mit der Legacy Darstellung.

3.2.4. Entscheidungssituation und gewählte Applikationen

Wie bereits in bei der Beschreibung der untersuchten Darstellungen (vgl. Kapitel 3.2.1 ab Seite 32) beschrieben, unterscheiden sich die verschiedenen Darstellungen in Hinblick auf den Umfang der zur

[28] Als bessere Leistung wird in diesem Kontext eine bessere Qualität der Entscheidung definiert, im Rahmen dieser Studie also die Wahl der Privatsphäre-freundlichsten Alternative, da andere Variablen (z.B. Anwenderbewertung oder Funktionalität) über die Alternativen weitestgehend konstant gehalten werden

Tabelle 2. Zusammenfassung der drei Entscheidungssituationen in der Evaluationsstudie

Kategorie	Hauptcharakteristiken	Beste Entscheidung*
Sudoku – einfache Entscheidung	• Applikation geringer Komplexität • Geringe Anzahl von Berechtigungen • Einfaches Muster von akzeptablen Berechtigungen, da keine funktionalen Gründe für den Zugriff auf persönliche Daten	Applikation mit den wenigsten Berechtigungen
E-Mail – komplexe Entscheidung	• Applikation hoher Komplexität • Größere Anzahl von Berechtigungen • Komplexes Muster von akzeptablen Berechtigungen, da funktionale Gründe für den Zugriff auf persönliche Daten	Applikation mit den wenigsten Berechtigungen
QR-Code-Scanner – täuschende Entscheidung	• Applikation mittlerer Komplexität • Mittlere Anzahl von Berechtigungen • Komplexes Muster von akzeptablen Berechtigungen, da funktionalen Gründe für den Zugriff auf persönliche Daten • Komplexe Entscheidung, da Applikation mit geringster Anzahl an Berechtigungen eine invasive Kombination von Berechtigungen hat	Applikation ohne invasive Berechtigungskombination, d.h. hier die Applikation ohne Zugriff auf Kommunikationskanäle (WLan, mobiles Internet o.ä.)

* in Hinblick auf die Privatsphäre

Verfügung gestellten Informationen. Einige sind, in Relation zur Legacy Android Darstellung, Zusammenfassungen (Kraus et al. [27], Kelley at al. [26] sowie Android 5.x), andere stellen zusätzliche Informationen bereit (Lin et al. [28] und COPING). Um die Qualität der Applikationswahl der Teilnehmer zu untersuchen, wurden insgesamt drei verschiedene Situationen konstruiert, jede repräsentiert durch eine Kategorie von Applikationen (vgl. Tabelle 2).

In jeder Kategorie wurden zufällig Logos von wenig populären Applikationen des Play Stores genommen, um ein Wiedererkennen möglichst unwahrscheinlich zu machen. Des Weiteren für jede Situation jeweils drei Applikationsbeschreibungen verfasst, die mit unterschiedlichen Formulierungen die gleiche Funktionalität beschrieben. Für jeden Probanden wurden diese dann zufällig einem Logo und Entwicklername zugeordnet. Die Reihenfolge der Situationen wurde ebenfalls für jeden Teilnehmer zufällig bestimmt.

Erste Situation. Diese wird durch drei verschiedene Sudoku-Applikationen (ein Logik-Spiel) konstruiert und repräsentiert eine *einfache Entscheidung* in Hinblick auf die Entscheidungsqualität. Das bedeutet, sie wurde so konstruiert, dass die korrekte, d.h. beste, Wahl in Relation zu den anderen beiden Situationen leichtfallen sollte. Dies wird erreicht durch den Fakt, dass es vergleichsweise einfach ist festzustellen, dass eine Sudoku Applikation für ihre Funktionalität keinerlei Berechtigungen benötigt. Jede Zugriffsanfrage auf persönliche Daten oder Kommunikationskanäle unterstützt nicht die Hauptfunktion der Applikation und somit ist, aus Sicht der Privatsphäre, die Alternative mit den wenigsten Berechtigungsanfragen die beste Alternative.

Zweite Situation. Diese wird durch drei verschiedene E-Mail-Applikationen konstruiert und repräsentiert eine *komplexe Entscheidung* in Hinblick auf die Entscheidungsqualität. Die Funktionalität einer E-Mail Applikation erfordert einige Berechtigungsanfragen für persönliche Daten (Kontakte) sowie Kommunikationskanäle (Internet), im Gegensatz zu den Sudoku-Applikationen der ersten Situation. Die angebotenen Alternativen sind hierbei so konstruiert, dass die beste, d.h. Privatsphäre-

freundlichste, Alternative jene mit den wenigstens Berechtigungen ist. Die zusätzlichen Berechtigungen sind klar nicht notwendig für die Kernfunktionalität der Applikation.

Dritte Situation. Diese wird durch drei verschiedene QR-Code-Scanner-Applikationen konstruiert und repräsentiert eine *täuschende Entscheidung* in Hinblick auf die Entscheidungsqualität. Sie repräsentiert eine Situation, in der ein Entwickler bewusst versucht, durch eine geschickte Wahl der angeforderten Berechtigungen und mit Kenntnis des Systems auf den Endanwender weniger gefährlich als vergleichbare Applikationen zu wirken und dennoch möglichst viele persönliche Daten zu sammeln. Die Komplexität der Applikationen ist geringer als bei den E-Mail-Applikationen, welche regulär Zugriff auf persönliche Daten und Kommunikationskanäle benötigen, jedoch höher als bei den Sudoku-Applikationen, welche gar keine Berechtigungen benötigen. Eine Applikation zum Scannen von QR-Codes benötigt ohne Frage den Zugriff auf die Kamera des Smartphones, um seine Kernfunktion zu erfüllen. Zumindest in Android besteht jedoch kein Grund für den Zugriff auf Kommunikationskanäle wie die Internetverbindung (über welche Daten abfließen könnten), da eine Applikation keine gesonderten Berechtigungen benötigt, um mit anderen Applikationen zu kommunizieren. Somit könnte ein aus einem QR-Code extrahierter Link problemlos über das Betriebssystem an die installierte Browser-Applikation weitergereicht werden, ohne dass die QR-Code-Scanner-Applikation vollen Netzwerkzugriff, inklusive aller damit verbundener Risiken, benötigt.

Insofern stellt hier die Applikation ohne Zugriff auf irgendwelche Kommunikationskanäle die, aus Perspektive der Privatsphäre, beste Entscheidung dar, nicht jene Applikation mit der geringsten Anzahl an Berechtigungen. Diese Konstruktion orientiert sich an der auch von Liccardi et al. [3] verwendeten Sensitivitätsbewertung in Hinblick auf die Privatsphäre. Um die beste Entscheidung in diesem Szenario zu treffen, ist also eine Bewertung der Kombination aus den angeforderten Berechtigungen notwendig. Ein einfaches Abzählen der Berechtigungen führt hier nicht zur korrekten Entscheidung. Eine informierte Entscheidung ist notwendig.

3.2.5. Ethik

Die Teilnehmer bekamen vor der Teilnahme eine Einverständniserklärung zu Fragen des Datenschutzes vorgelegt. Diese musste zunächst gelesen und akzeptiert werden, bevor eine Teilnahme möglich war. Alle Angaben können nicht mit der Identität der Teilnehmer in Verbindung gebracht werden und werden nur für wissenschaftliche Zwecke genutzt.

Darüber hinaus wurden alle Daten von SoSciSurvey in Deutschland auf deutschen Servern gespeichert und standen somit unter deutschem Datenschutzrecht. Erhobene Kontaktdaten, d.h. die E-Mail-Adresse, wurden, soweit durch den Teilnehmer angegeben, in einer gesonderten Datenbank gespeichert. Der Zweck war eine Verlosung unter allen Teilnehmern. Alle E-Mail-Adressen wurden nach der Verlosung direkt gelöscht.

Zum Abschluss der Studie wurden alle Teilnehmer über den Zweck der Studie aufgeklärt und erhielten zusätzlich weiterführende Informationen rund um Berechtigungen und die Änderungen an der Darstellung dieser im Play Store sowie die Risiken für die eigene Privatsphäre in Bezug auf Applikationen und Smartphones.

Tabelle 3. Zusammenfassung des Bildungsstandes und der Geschlechtsverteilung in der Stichprobe

		N	%
Geschlecht	Männlich	197	57,3
	Weiblich	139	40,4
	Anderes	8	2,3
Höchster Bildungsabschluss	Noch in der Schulausbildung	23	6,8
	Hauptschulabschluss	18	5,2
	Realschulabschluss	59	17,2
	(Fach-)Abitur	156	45,9
	Bachelor	40	11,8
	Master / Diplom / Magister (o.ä.)	29	8,5
	Promotion	7	2,1
	Anderer Abschluss	12	3,5
	Anderes	8	2,3

3.2.6. Stichprobe und Rekrutierung

Die Stichprobe wurde über eine Panel-Plattform mit dem Namen „Workhub“ rekrutiert. Diese stellte ein deutsches Äquivalent zu Amazons Mechanical Turk[29] dar. Zum Zeitpunkt des Verfassens der vorliegenden Arbeit ist das Unternehmen jedoch insolvent und nicht mehr verfügbar.

Die Stichprobe umfasst insgesamt 344 vollständige Teilnahmen zwischen September und Oktober 2014. Im Mittel waren diese 25,7 Jahre alt (SD = 8,3 Jahre), wobei der jüngste Teilnehmer 18 und der älteste 75 Jahre alt war. Die Geschlechterverteilung sowie der Bildungsstand sind in Tabelle 3 zusammengefasst. Insgesamt verfügten 255 (74,1%) der Teilnehmer über ein eigenes Android-Gerät. Im Mittel nutzen sie dieses für 13,8 Monate (SD = 15,4 Monate). Von den teilnehmenden 344 verfügten 59 (17,2%) über eine IT-orientierte Beschäftigung. Gemessen an der Gesamtbevölkerung in Deutschland liegt dieser Wert deutlich über dem Durchschnitt. In Deutschland gab es im Jahr 2015 insgesamt ca. 43 Millionen Erwerbstätige[30], wovon ca. 800.000 in der IT-Branche tätig waren[31], also ungefähr 2%.

Den Play Store besuchten 219 Teilnehmer (67,8%) zumindest zweimal pro Monat und 215 Teilnehmer (62,5%) hatten zwischen 10 und 50 Applikationen auf ihrem Gerät installiert. Abbildung 14 fasst das Nutzungsverhalten der Teilnehmer zusammen.

Von den zur Auswahl gestellten Applikationen erkannten 253 Teilnehmer (73,6%) keine wieder. Zumindest eine der Sudoku-Applikationen erkannten 12 Teilnehmer, 42 kannten zumindest eine der E-Mail-Applikationen und 61 zumindest eine der vorgeschlagenen QR-Code-Scanner-Applikationen.

[29] www.mturk.com/mturk/welcome

[30] https://www.destatis.de/DE/Publikationen/StatistischesJahrbuch/Arbeitsmarkt.pdf?__blob=publicationFile ; letzter Abruf 04.10.2017

[31] https://de.statista.com/statistik/daten/studie/186771/umfrage/erwerbstaetige-in-der-it-branche-in-deutschland/ ; letzter Abruf 04.10.2017

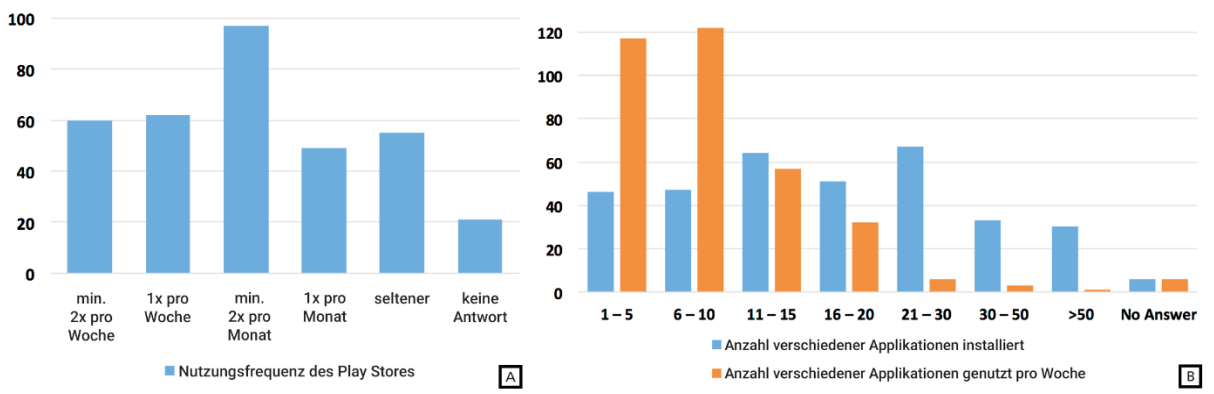

Abbildung 14. (A) Häufigkeit der Nutzung des Play Stores in der Stichprobe (B) Anzahl installierter und genutzter Applikationen auf dem eigenen Smartphone in der Stichprobe

3.2.7. Ergebnisse der Evaluation

Im Folgenden werden die Ergebnisse der Studie gruppiert nach den einzelnen Hypothesen dargestellt. Im Anschluss daran folgt die Diskussion und Einordnung in den Forschungskontext.

Da die „Privatsphärenfreundlichkeit" einer Applikation kein intervallskaliertes Merkmal in dieser Studie darstellte, konnte es auch nicht direkt als abhängige Variable für eine varianzanalytische Auswertung der Ergebnisse genutzt werden. Aus diesem Grund wurde zunächst für jeden Probanden die Häufigkeit einer korrekten Entscheidung, d.h. das Wählen der Privatsphären-freundlichsten Alternative, als intervallskaliertes Maß für die Effektivität der jeweiligen Berechtigungsdarstellung bestimmt.

Hypothese 1 – Gesamtanzahl Privatsphäre-freundlicher Entscheidungen. Für die erste Hypothese wurde jede Entscheidung jedes Teilnehmers, d.h. drei pro Teilnehmer, kodiert, je nachdem ob er die Privatsphäre-freundlichste (=1) oder nicht (=0) wählte. Daraus wurde dann die Gesamtsumme korrekter Entscheidungen für jeden Teilnehmer bestimmt, d.h. wie häufig er oder sie sich in den gestellten drei Entscheidungen für die Privatsphären-freundlichste Applikation entschied.

Dieses Häufigkeitsmaß diente als abhängige Variable in einer einfaktoriellen Varianzanalyse mit den sechs verschiedenen Berechtigungsdarstellungen als unabhängiger Variable. Um die Hypothese zu prüfen wurden dann die einfachen Kontraste betrachtet, wobei die Legacy Android Darstellung als Kontrollgruppe diente. Das bedeutet, dass alle Darstellungen der Studie mit der Legacy Android Darstellung verglichen wurden. Den gleichen Vergleich hatten alle aus der Literatur entnommenen Darstellungen bereits in zumindest einer eigenen Studie bestanden, d.h. sie erwiesen sich als signifikant besser als die Legacy Android Darstellung.

Tabelle 4 zeigt die in dieser Analyse verglichenen Mittelwerte mit den zugehörigen Standardabweichungen in Klammern, wobei ein Pfeil nach oben einen signifikant größeren Wert, ein Pfeil nach unten einen signifikant kleineren Wert als die Kontrollgruppe anzeigt. Je größer der Mittelwert, desto häufiger wurde durch Teilnehmer mit dieser Darstellung in der jeweiligen Entscheidungssituation die korrekte Entscheidung getroffen.

Die einfachen Kontraste zeigen hierbei signifikante Unterschiede ($F = 5{,}48$; $p < 0{,}01$). Es zeigt sich, dass einzig die Teilnehmer mit der COPING Darstellung signifikant bessere ($p < 0{,}01$) Entscheidungen als jene mit Legacy Android Darstellung treffen, wenn man alle Entscheidungssituationen gemeinsam betrachtet (letzte Spalte in Tabelle 4). Das bedeutet, Hypothese 1 trifft nur für die Darstellung zu, die

Tabelle 4. Mittelwerte der Häufigkeit korrekter Entscheidung für jede Berechtigungsdarstellung und Entscheidungssituation; Standardabweichungen sind in Klammern, Pfeile nach oben zeigen einen signifikant größeren, Pfeile nach unten einen signifikant kleineren Wert verglichen mit der Kontrollgruppe an

	Sudoku Einfache Entscheidung	E-Mail Komplexe Entscheidung	QR-Code-Scanner Täuschende Entscheidung	Gesamt
Legacy Android*	,75 (0,78)	,75 (0,44)	,22 (0,42)	1,72 (,78)
Android 5.x	,71 (0,46)	↓,50 (0,50)	,17 (0,38)	1,38 (,75)
Kraus et al. [26]	↓,57 (0,50)	↓,55 (0,50)	↑,52 (0,50)	1,64 (1,15)
Kelley et al. [25]	↓,53 (0,50)	,62 (0,49)	,31 (0,47)	1,46 (,82)
Lin et al. [27]	,72 (0,45)	,75 (0,44)	,14 (0,35)	1,61 (,76)
COPING	,71 (0,46)	,76 (0,43)	↑,71 (0,46)	↑2,18 (,84)

*Kontrollgruppe für einfache Kontraste

die umfangreichsten Informationen zur Verfügung stellt. Die anderen Unterhypothesen müssen abgelehnt werden, da alle anderen Darstellungen keine signifikante Verbesserung gegenüber der Legacy Darstellung zeigen. Ein genauerer Blick auf die Ergebnisse zeigt sogar, dass die Teilnehmer mit der Darstellung von Android 5.x sogar tendenziell schlechtere Entscheidungen getroffen haben ($p = 0,052$).

Hypothese 1 – Anzahl Privatsphäre-freundlicher Entscheidungen pro Entscheidungssituation. Neben der Analyse der Gesamtperformance wurde auch die Entscheidungsqualität in den einzelnen Entscheidungssituationen untersucht. Hierzu wurde zunächst eine Varianzanalyse mit Messwiederholung berechnet um zu prüfen, ob die sechs Berechtigungsdarstellungen in den einzelnen Situationen Unterschiede hinsichtlich der Entscheidungsqualität zeigten. Der Innersubjekt-Faktor waren hierbei die drei Entscheidungssituationen bzw. die Wahl in diesen, als Zwischensubjekt-Faktor fungierten erneut die sechs Berechtigungsdarstellungen.

Es zeigt sich eine signifikante Interaktion zwischen beiden Faktoren ($F = 6,24$; $p < 0,01$). In Tabelle 4 findet sich die detaillierte Auflistung aller Mittelwerte und Standardabweichungen aller Darstellungen für alle Entscheidungssituationen.

Zur genaueren Untersuchung dieser allgemeinen Unterschiede wurde eine multivariate Varianzanalyse berechnet[32]. Als unabhängige Variable fungierten hierbei die drei Entscheidungssituationen und die sechs Berechtigungsdarstellungen, als abhängige Variablen erneut das Häufigkeitsmaß für korrekte Entscheidungen für jede einzelne Entscheidungssituation. Erneut wurden die einfachen Kontraste zum Testen der Hypothese für jede Entscheidungssituation genutzt.

In der einfachen Entscheidungssituation (Sudoku Applikation) zeigen die Teilnehmer mit den beiden weniger umfangreichen Darstellungen von Kelley et al. [26] und Kraus et al. [27] eine signifikant schlechtere Entscheidungsqualität ($p = 0,04$ und $p = 0,02$) als die Kontrollgruppe. Die beiden

[32] Da die berechneten Kontraste jeweils nur die Darstellungen innerhalb einer Entscheidungssituation (nicht über mehrere hinweg) vergleichen, sind die entsprechenden Messwerte als unabhängig zu betrachten und die berechnete MANOVA vermeidet so gut wie möglich eine Kumulierung des Fehlers erster Art.

umfangreicheren Darstellungen zeigen keine Unterschiede. Das gilt ebenso für die Darstellung von Android 5.x.

In der komplexen Entscheidungssituation (E-Mail) zeigen die Teilnehmer mit der Darstellung von Kraus et al. sowie mit der von Android 5.x eine signifikant schlechtere Entscheidungsqualität als die Kontrollgruppe. Alle anderen Darstellungen zeigen vergleichbare Werte wie die Kontrollgruppe.

In der täuschenden Entscheidungssituation (QR-Code-Scanner), in der jene Applikation ohne Zugriff auf Kommunikationskanäle die beste Wahl darstellte, zeigen Teilnehmer mit der Darstellung von Kraus et al. sowie mit der COPING Darstellung signifikant bessere Entscheidungsqualität als die Kontrollgruppe. Darüber hinaus zeigen die Teilnehmer mit der COPING Darstellung auch eine signifikant bessere Entscheidungsqualität als jene mit der Darstellung von Kraus et al. Die anderen Darstellungen zeigen vergleichbare Werte wie die Kontrollgruppe.

Hypothese 2 – Hilfreich-Bewertungen der Darstellungen. Die zweite Hypothese postuliert einen signifikanten Unterschied zwischen der Legacy Android Darstellungen und allen anderen in Bezug auf die Bewertung, wie hilfreich die jeweilige Darstellung empfunden wird. Die detaillierten Bewertungen zu jeder Berechtigungsdarstellung finden sich in Tabelle 5.

Um diese Hypothese zu testen wurde eine multivariate Varianzanalyse berechnet. Als unabhängige Variable fungierte hierbei Berechtigungsdarstellung, als abhängige Variablen die einer siebenstufigen Likert-Skala folgenden Werte für die subjektiven Bewertungen „Die Berechtigungsdarstellung …“ „… war verständlich“, „war hilfreich“ und „scheint meine Privatsphäre zu schützen“ sowie die Häufigkeitswerte für „Ich habe die Berechtigungsdarstellung gelesen“. Diese Werte wurden in Phase 4 der Studie erhoben (vgl. Kapitel 3.2.2 ab Seite 34).

Die Auswertung zeigt eine signifikant schlechtere Nutzungs- ($p = 0{,}026$), Hilfreich- ($p = 0{,}025$) sowie Schützend-Bewertung ($p = 0{,}016$) durch die Teilnehmer mit der Darstellung von Android 5.x in Relation zur Kontrollgruppe. Das Gleiche gilt für die von Kraus et al. vorgeschlagene Darstellung ($p = 0{,}002$; $p = 0{,}011$; $p = 0{,}011$), wie in Tabelle 5 zusammengefasst. Die Darstellungen mit umfangreicheren Informationen zeigen keine Verbesserung in Relation zur Kontrollgruppe sowie untereinander, sodass Hypothese 2 nur in Teilen bestätigt werden kann.

Tabelle 5. Häufigkeit, Mittelwerte und Standardabweichungen für die subjektiven Einschätzungen aller sechs Berechtigungsdarstellungen; Standardabweichungen sind in Klammern, Pfeile nach oben zeigen einen signifikant größeren, Pfeile nach unten einen signifikant kleineren Wert verglichen mit der Kontrollgruppe an

	Gelesen		Genutzt	Verständlich	Hilfreich	Schützend
	ja	nein				
Legacy Android*	48	3	5,78 (1,63)	5,60 (1,29)	5,65 (1,51)	6,15 (1,31)
Android 5.x	36	11	↓ 4,88 (2,22)	5,02 (1,61)	↓ 4,96 (1,80)	↓ 5,36 (1,78)
Kraus et al. [26]	47	11	↓ 4,65 (2,15)	5,17 (1,72)	↓ 4,90 (1,79)	↓ 5,38 (1,98)
Kelley et al. [25]	45	9	5,76 (1,74)	5,78 (1,41)	5,89 (1,38)	5,85 (1,37)
Lin et al. [27]	62	6	5,44 (1,97)	5,73 (1,52)	5,58 (1,51)	5,68 (1,66)
COPING	43	4	5,71 (1,74)	5,67 (1,26)	5,82 (1,38)	6,25 (1,20)

*Kontrollgruppe für einfache Kontraste

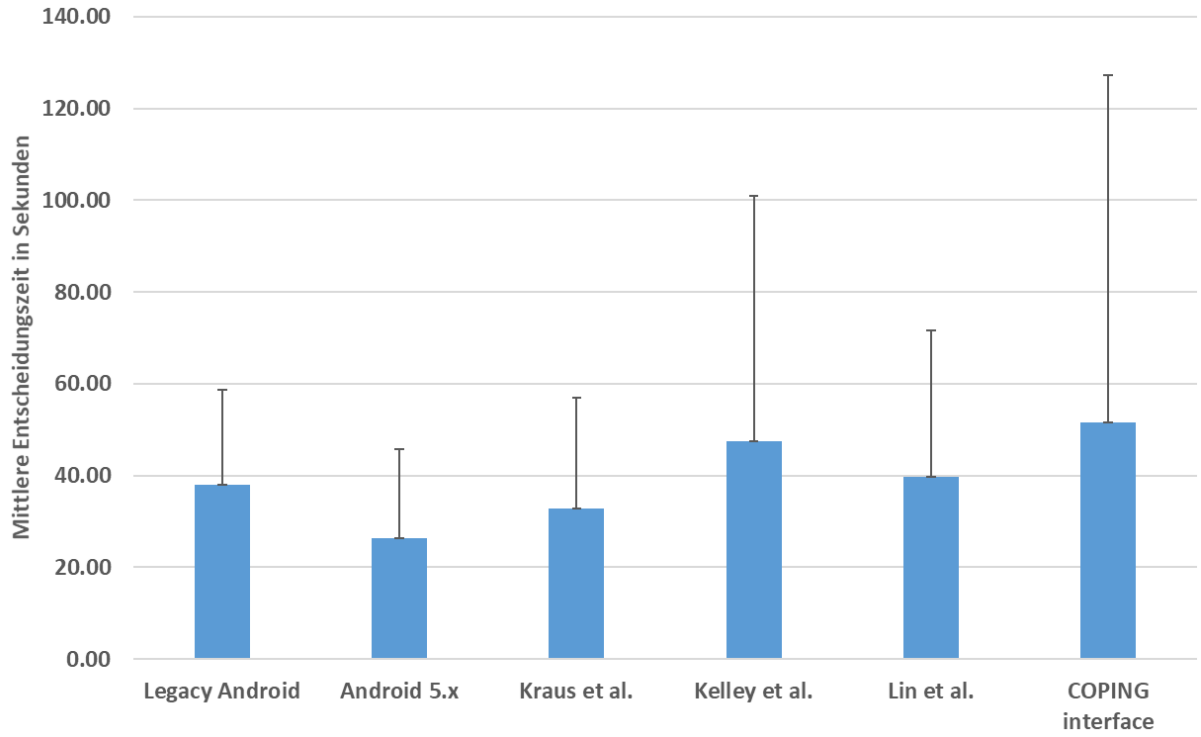

Abbildung 15. Mittlere Entscheidungszeiten in Sekunden über alle drei Entscheidungssituationen für die verschiedenen Berechtigungsdarstellungen mit markierten Standardabweichungen

Hypothese 3 – Dauer der Entscheidungen. Da die verglichenen Darstellungen unterschiedlich umfangreiche Informationen bereitstellen erscheint es plausibel, dass die Zeit bis sich die Teilnehmer für eine Applikation entschiedenen haben basierend auf der zugewiesenen Darstellung unterscheidet. Abbildung 15 bildet die mittleren Entscheidungszeiten für jede Darstellungsvariante ab. Obwohl der absolute Unterschied der mittleren Entscheidungszeiten zwischen der schnellsten Variante (Android 5.x mit M = 26,31; SD = 19,45) und der langsamsten (COPING mit M = 51,55s; SD = 75,67) groß wirkt, ist auch die Varianz sehr hoch.

Zur Untersuchung der dritten Hypothese wurde eine einfaktorielle Varianzanalyse mit der Berechtigungsdarstellung als unabhängiger Variable und der Entscheidungszeit als abhängiger Variable berechnet. Es zeigt sich, dass einzig der eben genannte extremste Unterschied signifikant wird ($F = 2{,}60$; $p = 0{,}03$). Alle anderen Unterschiede bleiben nicht signifikant, sodass die dritte Hypothese nur in Teilen bestätigt werden kann.

3.2.8. Diskussion der Ergebnisse

Die in anderen Studien berichteten Verbesserungen gegenüber der Legacy Android Darstellung [26–28] konnten in dieser Studie nicht repliziert werden. Einzig die Darstellung mit den umfangreichsten Informationen, der COPING Prototyp, konnte über alle Entscheidungssituationen hinweg signifikant bessere Entscheidungen der Teilnehmer vorweisen, während alle anderen mit der Kontrollgruppe vergleichbare oder schlechtere Ergebnisse zeigten. Ein genauerer Blick auf die verschiedenen Entscheidungssituationen zeigt, dass die Hauptunterschiede in der täuschenden Situation entstehen. In dieser kann die beste Entscheidung nicht durch simples Abzählen der angeforderten Berechtigungen getroffen werden. Die Art sowie die Kombination der Berechtigungen zu berücksichtigen ist hier für eine gute Entscheidung notwendig. Diese müssen also durch den Anwender verstanden und berücksichtigt werden.

Mit dieser Überlegung im Hinterkopf ist es plausibel, dass eine Abstraktion der Informationen, welche in der Android Legacy Darstellung geboten werden, wie sie zur Formulierung der weniger informationsreichen Darstellungen genutzt wird, auch zu einer schlechteren Entscheidungsqualität in Hinblick auf den Schutz der Privatsphäre führt. Der Vorschlag von Kraus et al. [27] bietet mit seinen statistischen Kennwerten die abstraktesten Informationen ohne die eigentlich angeforderten Berechtigungen überhaupt noch zu nennen. Wie invasiv eine Applikation für die eigene Privatsphäre ist, kann somit nur über einen Vergleich der Anzahl der geforderten Berechtigungen in Relation zum Mittel oder Quartil in der gleichen Kategorie eingeschätzt werden. Unsere Ergebnisse dokumentieren eine schlechtere Entscheidungsqualität als die Legacy Android Darstellung, sogar bei der einfachen Entscheidung über die Sudoku-Applikation. Signifikant schlechtere Bewertungen hinsichtlich dessen, wie hilfreich und schützend die Darstellung empfunden wird, scheinen den Eindruck zu erhärten, dass diese Art der Darstellung allein nicht für den täglichen Gebrauch geeignet ist.

Die „Privacy facts“ von Kelley et al. [26] bieten in Relation zum Vorschlag von Kraus et al. etwas umfangreichere, weil auch inhaltlich an den Berechtigungen angelehnte, Informationen. Verglichen mit der Legacy Android Darstellung ist sie aber immer noch abstrahierend. Die einzelnen Checkboxen mit Häkchen scheinen in der Tat eher ein Abzählen als ein sorgfältiges Vergleichen zu begünstigen, wie bereits Harbach et al. [29] anmerkten. Vergleichbar mit der Darstellung, welche in Android 5.x verwendet wird, fällt es dem Anwender schwer, zwischen Applikationen mit einer unterschiedlichen Anzahl von Berechtigungen in den selben Kategorien zu unterscheiden. Es scheint so, dass ein Anwender mit dieser Art von Darstellung nicht in der Lage ist, invasiv in die Privatsphäre eindringende Applikationen zu identifizieren, wenn die Berechtigungen bewusst durch den Entwickler gewählt werden. Dies zeigt sich in dem untersuchten täuschenden Entscheidungsszenario, in welchem die beste Entscheidung nicht jene mit den wenigsten Häkchen war.

Der von Lin et al. [28] gemachte Vorschlag zeigt eine vergleichbare Entscheidungsqualität wie die Legacy Darstellung von Android. Die zusätzlichen Informationen durch die Nutzereinschätzung der einzelnen Berechtigungen sowie die Warnzeichen für unerwartete Berechtigungen verstärkten nicht das Verständnis der Teilnehmer für das Berechtigungs-Set. Unsere Teilnehmer scheinen schlicht die Länge der Berechtigungslisten verglichen und sich häufig für die Applikation mit der kürzesten Liste entschieden zu haben (wie auch jene mit der Legacy Darstellung).

Einzig der COPING Prototyp, die Darstellung mit den umfangreichsten Informationen, bot genug verständliche Informationen über das Set der angeforderten Berechtigungen, sodass die Teilnehmer auch die täuschende Situation korrekt einschätzen konnten. Diese Darstellung zeigt eine signifikant verbesserte Entscheidungsqualität über alle drei Entscheidungen verglichen mit der Kontrollgruppe. Sie bietet somit auch eine bessere Entscheidungsqualität als die anderen untersuchten Darstellungen, da diese alle auf einem vergleichbaren oder schlechteren Niveau als die Kontrollgruppe agieren.

Dennoch steigen die Kosten, hier in Form der Zeit sich zu entscheiden, nicht signifikant an. Es konnten mit Ausnahme der Android 5.x Darstellung keine signifikanten Unterschiede hinsichtlich der Entscheidungszeit festgestellt werden, welche jedoch gleichzeitig signifikant schlechtere Ergebnisse lieferte. Gleichzeitig sind die mittleren Entscheidungszeiten dennoch so hoch, dass es plausibel erscheint, dass die Teilnehmer nicht schlicht auf das initiale Gesamturteil der Experten (ob das Set an geforderten Berechtigungen angemessen erscheint oder nicht) allein vertraut haben, sondern die detaillierteren Informationen der Darstellung, warum das so ist, gelesen und in der Entscheidung berücksichtigt haben.

Felt et al. [20] berichteten, dass etwa 20% der von ihnen erhobenen Stichprobe „Experten-Anwender“ waren und kamen zu dem Schluss, dass genau diese anderen Anwendern helfen könnten, indem sie Reviews schreiben oder Bewertungen abgeben, wenn sie auf unangemessene Berechtigungen bei einer Applikation aufmerksam werden. Dies würde ohne Frage jenen Anwendern helfen, die lieber auf die Bewertungen anderer Anwender vertrauen, als selbst zu versuchen die Berechtigungen einzuschätzen. Um die Daten für eine Darstellung wie COPING zu generieren, erscheint ein Crowd-Sourcing Ansatz, ähnlich wie bereits Lin et al. [28] ihn nutzte, vielversprechend. In einem solchen sollte zunächst das Wissen über und das Verständnis für das Berechtigungssystem geprüft werden, ähnlich wie auch Felt et al. es in ihrer Studie taten. Im Anschluss daran sollten die Applikationen sowie die zugehörigen Berechtigungsanforderungen gezeigt und durch die Teilnehmer hinsichtlich ihrer Angemessenheit in Bezug auf die gebotene Funktionalität bewertet werden.

Da viele Anwender Berechtigungen nicht gut verstehen, wie bereits von vielen Forschern gezeigt wurde (z.B. [18], [19], [25]), versuchen viele alternative Vorschläge für Berechtigungsdarstellungen den Umfang der dargestellten Informationen zu reduzieren, um auf diesem Wege das Interface zu vereinfachen. Die Änderungen, die Google an der Darstellung der Berechtigungen in Android für die Versionen bis einschließlich 5.x vornahm, scheinen exakt dieser Leitlinie zu folgen und führen zu einer abstrakteren Informationsdarstellung. Anstatt den Anwender durch bessere Werkzeuge in die Lage zu versetzen, Risiken besser zu verstehen und in seinen Entscheidungen zu berücksichtigen, führen solcher Art abstrahierte Darstellungen zu einer Situation, in der viele Anwender nur noch Häkchen zählen oder die Länge von Listen vergleichen. Eine solche „je weniger desto besser“ Heuristik, welche passend im Szenario mit der täuschenden Entscheidung illustriert wurde, kann sehr einfach durch jede Entität ausgenutzt werden. Eine solche Entität kann die Berechtigungen bewusst so wählen, dass sie den abstrakten Repräsentationen passt, jedoch Zugriff auf viele persönliche Daten erlaubt.

Dies trifft in besonderem Maße auf die Darstellung in Android 5.x zu, welche die schlechteste Entscheidungsqualität in dieser Studie zeigte. Diese erhielt auch vergleichsweise schlechte Bewertungen hinsichtlich dessen, wie hilfreich und schützend diese Darstellung wahrgenommen wird und wie sehr die Informationen in den Entscheidungen berücksichtigt wurden. Die Entscheidungszeit sank in Relation zur Darstellung mit den umfangreichsten Informationen, aber dies geht klar zu Lasten der Güte der getroffenen Entscheidungen.

Zusätzlich sollte angemerkt werden, dass die hier verwendete Darstellung von Android 5.x einen „Best-case“ darstellt, da die detaillierte Version genutzt wurde, welche nur über einen kleinen Link am unteren Ende der Applikationsdetailseite im Play Store verfügbar ist. Die Darstellung, welche regulär beim Betätigen des Installieren- bzw. Aktualisieren-Buttons erscheint, beinhaltet nicht die Berechtigungsgruppe „Sonstige“, welche einige der invasiveren Berechtigungen wie „Voller Internetzugriff“ oder „Gespeicherte Konten nutzen“ enthält. Selbst wenn eine neue Version einer Applikation (weitere) Berechtigungen aus dieser Kategorie anfordert, wird diese dennoch nicht angezeigt [21].

Dies gilt auch für die Darstellung in Android 6.0 oder iOS, welche gar keine Anzeige der Berechtigungen bei der Installation mehr haben. iOS verzichtet im App Store sogar vollständig auf eine Erwähnung dieser. Das Anfordern von Berechtigungen während der Laufzeit bietet Vorteile, wie z.B. die möglicherweise bessere Verknüpfung zwischen Funktionalität und Berechtigung, aber es hat auch Nachteile. Bereits gewährte Berechtigungen werden in beiden Implementierungen nicht erneut angezeigt und können nicht temporär gewährt werden, sodass sie beispielsweise nach einer

Anwendung oder einem bestimmten Zeitintervall erneut angefordert werden müssen. Eine Einschätzung der Risiken, welche durch mögliche Interaktionen zwischen Berechtigungen entstehen können erscheint in diesen Darstellungen sehr schwer möglich.

Dennoch bieten die durch Android 6.0 bzw. in iOS gebotenen Kontrollmechanismen einzelner Berechtigungen durchaus Vorteile, wie die Untersuchung von Wang et al. [30] zeigte. Hier wurde zwar auch mit der Legacy Android Darstellung verglichen, jedoch erscheint eine Kombination der von den neueren Android Versionen bzw. von iOS gebotenen Kontrollmechanismen und der umfangreichen und strukturierten Darstellung von COPING vor diesem Hintergrund sehr vielversprechend.

3.2.8.1. Limitationen

Eine der wichtigsten Limitationen der hier vorgestellten Studie stellt die Abwesenheit von wirklich realem Verhalten dar. Die Teilnehmer mussten die gewählten Applikationen nicht auf dem eigenen Gerät installieren und nutzen, sondern bearbeiteten ein rein hypothetisches Szenario. Zusätzlich wurde im Rahmen der Studie ein Side-by-Side Vergleich mehrerer Applikationen geboten, welcher in dieser Form zumindest im Moment von keinem bekannten öffentlich verfügbaren Store für Applikationen angeboten wird. Andererseits sind die Angebote für Smartphone Applikationen nicht auf dasselbe beschränkt[33], sondern können auch mittels Browser an Geräten mit größeren Bildschirmen genutzt werden, um Applikationen zu wählen und direkt auf verknüpfte Geräte zu pushen. Insofern ist ein Side-by-Side Vergleich ähnlich zur hier vorgestellten Studie nicht völlig undenkbar.

In Bezug auf die Bewertung einer einzelnen Applikation, wie es auf einem Smartphone wohl am wahrscheinlichsten ist, nutzt der Entwurf des COPING Prototypens den gleichen horizontalen Platz sowie die gleiche Schriftart und -größe wie alle anderen Darstellungen inklusive der Android-eigenen. Somit gibt es keinen augenscheinlichen Grund, warum diese Art der Darstellung nicht auch auf kleineren Bildschirmen verwendet werden sollte.

Des Weiteren stand den Teilnehmern nur ein Nachbau des Google Play Stores zur Entscheidungsfindung zur Verfügung, welcher weniger dynamische Inhalte als das Original bot. Auf Grund technischer Beschränkungen seitens der Umfrageplattform waren die Applikationsdetailseiten nur zusammengesetzte statische Bilder ohne die ggf. vom Play Store gewohnten interaktiven Möglichkeiten. Außerdem wurden die Beschreibungen der Applikationen gekürzt, sodass diese nur die Kernfunktionen der Applikationen skizzieren. Andere typische Bestandteile, wie z.B. eine Liste der Funktionen oder ein Protokoll der Änderungen durch das letzte Update, waren nicht Teil der Studie, da sie normalerweise keine für die Privatsphäre bedeutsamen Informationen enthalten.

In der Studie kam nur eine kleine Stichprobe von verfügbaren Applikationen und -kategorien zur Anwendung. Dies begrenzt die Generalisierbarkeit der Ergebnisse. Ebenso wurden die Darstellungsmodi von Android 6.0 und iOS nicht untersucht. Der in ihnen enthaltene Wechsel der Paradigmen von „vor der Installation“ zu „während der Laufzeit“ erfordert ein gänzlich anderes Studiendesign.

Schließlich besteht die untersuchte Stichprobe einzig aus deutschsprachigen Teilnehmern, was verhindert, dass kulturelle Effekte näher betrachtet werden können. Aus diesem Grund wurden

[33] Dies trifft zumindest auf den Google Play Store sowie den App Store von Apple zu

bewusst umfangreiche demographische Informationen sowie Daten zum typischen Nutzerverhalten der Stichprobe mit berichtet, um eine Replikation und kulturelle Vergleiche zu ermöglichen.

Abschließend bleibt festzuhalten, dass mit dem COPING Prototypen die Darstellung die besten Ergebnisse zeigte, welche auch die umfangreichsten Informationen zur Verfügung stellt. Dies liefert keine Information darüber, ob eine Darstellung mit noch umfangreicheren Informationen nicht unter Umständen noch bessere Ergebnisse liefern würde. Insofern kann nicht behauptet werden, dass die COPING Darstellung die optimale ist, nur, dass sie besser als die anderen untersuchten funktioniert.

3.3. Fazit für das weitere Vorgehen

Anwender nutzen für ihre Entscheidungen darüber, ob sie eine Applikation oder einen Dienst installieren wollen, die verschiedensten Informationen. Hierzu gehören direkt Privatsphäre-relevante Informationen, wie im mobilen Bereich die Berechtigungen, die eine Applikation anfordert. Hierbei spielt es eine entscheidende Rolle, wie umfangreich die Informationen sind und vor allem auch, wie diese aufbereitet werden. Jedoch erklären die reinen Unterschiede hinsichtlich der Berechtigungen nicht vollständig das Wahlverhalten der Studienteilnehmer. Es erscheint also offensichtlich, dass auch andere Informationen genutzt werden, welche zum Teil auch gar nichts direkt mit der Privatsphäre zu tun haben. Selbst in der Evaluationsstudie, in welcher Funktionalität, Nutzerbewertungen und Entwickler kontrolliert wurden, wählten fast 30% der Teilnehmer unabhängig von der zugewiesenen Darstellung nicht die Privatsphäre-freundlichste Alternative.

Dies wirft die Frage auf, welche Faktoren genau eine Rolle bei der Entscheidungsfindung spielen und wie diese zusammenhängen. Die bisher gewonnenen Erkenntnisse liefern uns qualitative Einblicke darin, welche Faktoren dafür in Frage kommen (vgl. Kapitel 2.1.3 ab Seite 14) können, jedoch bieten sie keine Informationen zur Struktur dieser Faktoren. Auch eine Gewichtung, d.h. welche Faktoren besonders relevant bei Privatsphäre-bezogenen Entscheidungen sind, ist bisher nicht ableitbar.

Zum Formulieren eines strukturierten Verhaltensmodells gilt es also zunächst Erkenntnisse zu Zusammenhängen zwischen den einzelnen Faktoren zu sammeln. Hierzu gibt es bereits eine Vorarbeit von Gerber et al. [35], in der nach einer umfangreichen Literaturrecherche diverse Faktoren, welche für die Verhaltensbildung bei Privatsphäre-relevanten Entscheidungen eine Rolle spielen, zusammengetragen wurden. Aufbauend auf diesen literaturbasierten und den bisherigen empirischen Erkenntnissen soll deshalb im folgenden Kapitel ein integratives Verhaltensmodell formuliert und empirisch überprüft werden.

4. Entscheidungsfaktoren im Kontext Privatsphäre-relevanten menschlichen Verhaltens

Eine der einflussreichsten Theorien aus der psychologischen Forschung zum menschlichen Verhalten ist die sogenannte Theorie des geplanten Verhaltens (engl.: Theory of planned behavior) [36]. Diese zeigt auf, dass das Verhalten eines Menschen nicht ausschließlich von dessen Motivation, bzw. Intention, dieses zu zeigen abhängt. Die Theorie des geplanten Verhaltens versucht hierbei allgemein menschliches Verhalten in einer gegebenen Situation zu erklären (vgl. Abbildung 16).

Als einer der Antezedenzien für gezeigtes Verhalten ist hierbei die Absicht bzw. die Intention (d.h. die jeweilige Person ist willens, sich in einer gegebenen Situation entsprechend zu verhalten) ein wichtiger Teil der Theorie. Die Verhaltensabsicht jedoch ist wiederum abhängig von der (positiven oder negativen) Einstellung dem entsprechenden Verhalten gegenüber. Zusätzlich wirkt eine subjektive Norm auf die Intention, welche ein soziales Konstrukt darstellt und stellvertretend für einen subjektiven Druck, ein bestimmtes Verhalten (nicht) zu zeigen, steht. Schließlich wirkt noch die wahrgenommene, d.h. subjektive, Erfolgswahrscheinlichkeit auf die Bildung einer Verhaltensabsicht. Unter ihr versteht man den Grad an Überzeugung in einer gegebenen Situation ein spezifisches Verhalten erfolgreich durchzuführen, womit sie ein Maß für die subjektive Einfachheit bzw. Schwierigkeit eines Verhaltens ist. Diese subjektive Einfachheit oder Erfolgswahrscheinlichkeit hat einen Einfluss darauf, welche möglichen Verhaltensalternativen gewählt werden, wie viele Ressourcen (d.h. zeitlicher oder finanzieller Art) in die Aufrechterhaltung des Verhaltens investiert werden sowie hiermit verknüpfte emotionale Reaktionen, wie beispielsweise Stolz [37–39].

Diese Theorie greift grundlegende Konstrukte der Verhaltensbildung bereits auf, es fehlen jedoch für den Kontext dieser Arbeit weitere Konstrukte, z.B. das Risiko, d.h. die Komponente der möglichen negativen Konsequenzen. Neben der Wahrnehmung des Risikos selbst, d.h. den mit einem Verhalten potentiell verbundenen negativen Konsequenzen, ist verhaltenspsychologisch insbesondere interessant, wie der Mensch versucht, mit diesen umzugehen, sie zu vermeiden oder auch die Wahrscheinlichkeit des Auftretens oder die Schwere der Auswirkungen zu reduzieren.

Ursprünglich aus dem Feld der Gesundheitspsychologie stammt hierzu die Schutz-Motivations-Theorie (engl.: Protection motivation theory) von Rogers [40] bzw. Floyd und Kollegen [41]. Diese versucht, sowohl auf individueller wie auch gesellschaftlicher Ebene Verhaltensabsichten hinsichtlich des

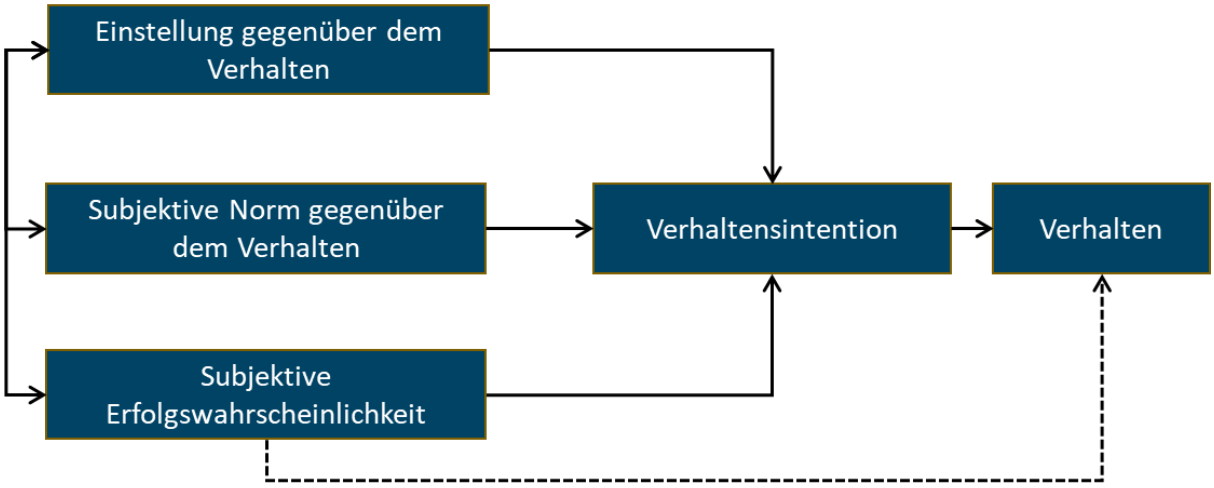

Abbildung 16. Schematische Darstellung der Theorie des geplanten Verhaltens

Gesundheitsschutzes mittels zweier Faktoren vorherzusagen, der Bedrohungseinschätzung und der Bewältigungseinschätzung.

Bei der Bedrohungseinschätzung werden die wahrgenommene Schwere sowie die wahrgenommene Wahrscheinlichkeit der (gesundheitlichen) Bedrohung miteinander verbunden. Bei der Bewältigungseinschätzung wird zum einen die Effektivität der möglichen präventiven Handlung und zum anderen die jeweilige wahrgenommene Fähigkeit, die präventive Handlung erfolgreich durchzuführen, genutzt. Beide Prozesse nutzen zusätzlich noch vorhandene Informationen aus der direkten Umgebung (beispielsweise Überredung durch Angehörige) sowie personenbezogene Eigenschaften wie frühere Erfahrungen, um eine kombinierte Schutzmotivation zu formen.

Darüber hinaus gibt es noch weitere Verhaltenstheorien, die sich noch näher mit dem Gegenstand dieser Arbeit, dem Entscheiden in Privatsphäre-relevanten Situationen, beschäftigen. Hierzu gehören vor allem auch die verschiedenen Theorien, die sich dem Privacy Calculus (z.B. [42], [43]) genannten Rahmenwerk zuordnen lassen. Diese folgen der Grundannahme eines Menschen, der versucht einen möglichst optimalen Kompromiss zwischen möglichen Risiken und potentiellen Vorteilen, die mit einer Handlung verknüpft sind, zu finden. Ein Beispiel hierfür ist die Theorie der Nutzenmaximierung (engl.: Utility maximization theory) von Rust und Kollegen [44] bzw. Awad und Krishnan [45].

Keine dieser eher allgemeinen Verhaltenstheorien erfasst jedoch alle spezifischen Gegebenheiten der Verhaltensbildung im digitalen Alltag. In jeder dieser Theorien finden jeweils verschiedene Faktoren die, wie bereits in früheren Kapiteln dieser Arbeit beobachtet, für Entscheidungen eine Rolle spielen, keine Berücksichtigung. Sei es beispielsweise die Reputation und Vertrauenswürdigkeit des Entwicklers einer Applikation oder z.B. die subjektive Sicherheit einer Applikation, die an Hand der Regelmäßigkeit von Updates abgeschätzt werden kann (vgl. Kapitel 2.1.3 ab Seite 14).

Das übergeordnete Ziel dieses Kapitels besteht darin, diese spezifischen Faktoren zu sammeln und zu strukturieren, um ein integratives Verhaltensmodell zu formulieren, welches die Entscheidungsfindung im digitalen Alltag besser abbilden kann.

Insofern werden für das aktuelle Kapitel folgende Ziele formuliert:

1. Identifikation relevanter Einflussfaktoren für menschliches Handeln im digitalen Alltag bzw. am Smartphone auf Basis des Standes der Forschung
2. Integration bisheriger empirischer Erkenntnisse, insbesondere der Heuristiken
3. Formulierung eines integrativen Verhaltensmodells für den digitalen Alltag als Forschungsmodell in Form eines Strukturgleichungsmodells
4. Evaluierung und Bewertung des Forschungsmodells
5. Abschätzung der relativen Bedeutsamkeit gefundener Faktoren

Das vorliegende Kapitel ist, diesen Zielen folgend, so strukturiert, dass zunächst die Methodik der durchgeführten Literaturanalyse kurz skizziert wird. Auf deren Ergebnissen wird im darauffolgenden Unterkapitel aufbauend das integrative Verhaltensmodell formuliert und im Anschluss anhand der empirischen Erkenntnisse der vorherigen Kapitel bewertet. Danach wird eine Studie zur Überprüfung des Modells vorgestellt, um das Kapitel mit der Diskussion und Interpretation der dokumentierten Ergebnisse zu schließen.

4.1. Identifikation relevanter Literatur

Die hier diskutierten Inhalte basieren auf einer umfangreichen Literaturanalyse zwischen November 2015 und Februar 2016. Hierbei wurden die Datenbanken von Google Scholar, ACM, IEEE und Scopus mit dem Stichwort „Privacy Paradox" nach englischsprachigen Publikationen durchsucht. Der Zeitraum der Publikation für die direkten Treffer wurde dabei auf 2006 bis 2016 begrenzt. Relevant waren hierbei Publikationen, die sich direkt oder indirekt mit dem Suchgegenstand beschäftigen, d.h. ihn entweder direkt untersuchten, oder im Rahmen ihrer Überlegungen und/oder Studien Beobachtungen machten, die damit zusammenhängen. In einem weiteren Schritt wurden die Literaturverzeichnisse der relevanten Publikationen für eine weiterführende Vorwärts- und Rückwärtssuche genutzt. Hierbei lag der Fokus primär darauf, Originalquellen für genutzte und/diskutierte Modelle und Theorien zu identifizieren, deren Publikationsdatum außerhalb des zunächst genutzten Zeitraums liegt.

4.2. Formulierung eines integrativen Verhaltensmodells

Im Folgenden wird jeder Faktor im Modell hypothesenorientiert inhaltlich beschrieben. Dabei wird zunächst das Konstrukt selbst beschrieben, um danach die Effekte, die es auf andere Konstrukte hat, zu beschreiben und schließlich als Hypothese zu formulieren. Das Kapitel schließt mit einer Einordnung der in Kapitel 2.1.3 formulierte Heuristiken zur Applikationsauswahl in das Forschungsmodell.

4.2.1. Forschungshypothesen

In diesem Unterkapitel werden die insgesamt 30 Hypothesen des Forschungsmodells inhaltlich erläutert und formuliert. Am Ende des Kapitels werden diese in einer schematischen Übersicht zum leichteren Verständnis visualisiert (vgl. Abbildung 17).

Jahre der Internetnutzung & Anzahl genutzter Onlinedienste. Der Mensch sammelt im Laufe seines Lebens die verschiedensten Erfahrungen und lernt aus diesen, wie er sich in verschiedenen Situationen erfolgreich verhalten kann. Das gilt natürlich auch für den digitalen Alltag, d.h. die Nutzung des Internets [46]. Je nachdem, wie erfolgreich jemand ist, steigen dabei die Fähigkeiten und auch die Überzeugung, diese erfolgreich in weiteren Situationen anwenden zu können. Dabei spielt auch die Intensität, sei es Dauer oder Häufigkeit, eine große Rolle [47].

> *H_1: Die Anzahl der Jahre, die eine Person bereits Erfahrung mit dem Internet gesammelt hat, hat einen signifikant positiven Einfluss auf das Selbstbewusstsein.*

> *H_2: Die Anzahl der genutzten Onlinedienste, die eine Person nutzt, hat einen signifikant positiven Einfluss auf das Selbstbewusstsein.*

Im Umkehrschluss gilt, wer wenig Erfahrung oder Wissen aufweist, traut sich eher weniger zu, insbesondere im komplexen Online-Kontext.

> *H_3: Die Anzahl der Jahre, die eine Person bereits Erfahrung mit dem Internet gesammelt hat, hat einen signifikant negativen Einfluss auf die Computerängstlichkeit.*

> *H_4: Die Anzahl der genutzten Onlinedienste, die eine Person nutzt, hat einen signifikant negativen Einfluss auf die Computerängstlichkeit.*

Frühere Erfahrungen mit Onlinediensten. Frühere Erfahrungen mit Onlinediensten können sowohl positiver, als auch negativer Natur sein. Wenn ein Dienstleister sich an Absprachen hält oder der Dienst wirklich nützlich für einen ist, so hat der Anwender eher positive Erinnerungen an die Nutzung. Bekommt er jedoch plötzlich deutlich mehr Spam-E-Mails oder Werbebriefe, nachdem er einem Dienstleister seine Kontaktdaten zur Verfügung gestellt hat, kann dies schnell zu einer eher negativen Erfahrung führen. Dabei stehen positive Erfahrungen, insbesondere erfolgreiche Handlungen oder Aktivitäten eher mit der Bildung eines positiven Selbstwertes bzw. der Steigerung des Selbstbewusstseins in Verbindung [48].

H_5: Die positiven früheren Erfahrungen mit Onlinediensten, die eine Person gemacht hat, haben einen signifikant positiven Einfluss auf das Selbstbewusstsein.

Entsprechend wirken negative Erfahrungen eher auf die Sorge, dass Dinge, die man angeht, eher schiefgehen oder negative Konsequenzen den eigenen Handlungen folgen.

H_6: Die negativen früheren Erfahrungen mit Onlinediensten, die eine Person gemacht hat, haben einen signifikant negativen Einfluss auf die Computerängstlichkeit.

Selbstbewusstsein. Das Selbstbewusstsein des Menschen beinhaltet Gefühle des Selbstwertes und Selbstrespektes [49]. Es stellt die Manifestation der Selbstbewertung eines Individuums dar [50], da es die generelle Einschätzung der eigenen Person widerspiegelt [51]. Entsprechend steht es in Zusammenhang mit anderen internen Selbstbewertungsmechanismen, wie der Selbstwirksamkeit [37], [39] bzw. der subjektiven Kontrolle [36].

H_7: Das Selbstbewusstsein einer Person hat einen signifikant positiven Einfluss auf die subjektive Kontrolle.

Ein schwaches Selbstbewusstsein geht normalerweise mit einem eher zurückhaltenden Verhalten einher [52], es ist also zu vermuten, dass ein niedriges Selbstbewusstsein mit einem erhöhten Bedürfnis nach Privatsphäre einhergeht [53].

H_8: Das Selbstbewusstsein einer Person hat einen signifikant negativen Einfluss auf die spezifischen Privatsphäre-Bedenken.

Computerängstlichkeit. Trotz, oder gerade wegen, der rasanten Verbreitung von Smartphones in den letzten zehn Jahren gibt es dennoch Menschen, die Technik eher meiden, sei es aus Angst etwas falsch zu machen und Beschädigungen hervorzurufen oder aus Sorge über die Folgen fortschreitender Automatisierung und Kontrollverlust [54]. Entsprechend gehen Menschen mit niedrigen Werten in Computerängstlichkeit souveräner und routinierter mit Computern und Technik im Allgemeinen um und erwarten eher erfolgreich zu sein bzw. nicht zu scheitern. Während das Selbstbewusstsein eher eine generelle Einschätzung der eigenen Person darstellt [51], bezieht sich die Computerängstlichkeit direkt auf die eigene Einschätzung hinsichtlich von Computern bzw. Technik.

H_9: Computerängstlichkeit einer Person hat einen signifikant negativen Einfluss auf die subjektive Kontrollüberzeugung.

Schwaig et al. [53] zeigten, dass jene Menschen, die Sorge haben um die Wechselwirkung zwischen Gesellschaft und Technik, insbesondere in Hinblick auf Automatisierung und unsichtbare Datenflüsse, eher negativ auf Datensammlung reagieren. Die Verbreitung persönlicher Daten durch die breite

Nutzung von Technik und Automatisierung fördert bei Menschen mit hohen Ausprägungen von Computerängstlichkeit also Sorgen und Bedenken.

H_{10}: Personen mit hohen Werten von Computerängstlichkeit haben auch erhöhte spezifische Privatsphäre-Bedenken.

Konsumentenentfremdung. Konsumenten Entfremdung beschreibt das Phänomen, dass Menschen sich fremd in Bezug auf den Markt fühlen. Sie fühlen, dass ihre persönlichen Werte und Bedürfnisse nicht mehr denen entsprechen, die auf dem Markt vorherrschen und üblich sind. Der Markt selbst umfasst dabei alle Institutionen, die direkt oder indirekt am Angebot von Waren und Dienstleistungen beteiligt sind, d.h. beispielsweise Hersteller, Vertrieb aber auch Marketing [55]. Menschen, die sich vom Markt als solchem entfremdet fühlen und die ihre persönlichen Wertvorstellungen und Bedürfnisse nicht mit denen des Marktes als übereinstimmend wahrnehmen, stehen diesem und seinen Angeboten eher ablehnend gegenüber [56–58].

H_{11}: Die Konsumentenentfremdung einer Person hat einen signifikant negativen Einfluss auf die Einstellung.

Das Gefühl der Entfremdung geht häufig auch mit einem Gefühl der Machtlosigkeit einher. Dieses führt dazu, dass Menschen nicht glauben, erfolgreich Einfluss auf den Markt und dessen Verhalten bzw. Werte nehmen zu können, um diesen im Sinne der eigenen Werte und Bedürfnisse zu verändern [57].

H_{12}: Die Konsumentenentfremdung einer Person hat einen signifikant negativen Einfluss auf die subjektive Kontrollüberzeugung.

Subjektive soziale Norm. Die subjektive soziale Norm steht für die Normen und Anforderungen und Werte, die das soziale Umfeld subjektiv an ein Individuum stellt und ist Teil der Theorie des geplanten Handelns [36]. Diese Normen und Anforderungen müssen dabei nicht tatsächlich genau so formuliert und existent sein, die Wahrnehmung durch das Individuum selbst genügt hierbei. Zum sozialen Umfeld gehören dabei sowohl Freunde und Familie als auch das Arbeitsumfeld oder auch Vorbilder, die bestimmte Werte vorleben. Was subjektiv Freunde, die Familie oder auch Arbeitskollegen als gut, richtig und/oder wichtig wahrnehmen, wird auch durch das betreffende Individuum als positiver wahrgenommen. Das gleiche gilt auch für den umgedrehten Fall einer negativen Wahrnehmung. Die Einstellung gegenüber einer Verhaltensweise oder einer Entität wird also von der subjektiven sozialen Norm, d.h. was glaubt das Individuum wie andere, ihm wichtige, Personen darüber denken, beeinflusst.

H_{13}: Die subjektive soziale Norm einer Person hat einen signifikant positiven Einfluss auf die Einstellung.

Subjektive Sensitivität der Daten. Die individuelle Bewertung von Daten beinhaltet nicht nur, wem diese Daten zu welchem Zweck zur Verfügung gestellt werden, sondern auch, um welche Daten es sich überhaupt handelt. Es macht einen Unterschied, ob es sich um beispielsweise allgemeine demographische Daten wie beispielsweise das Geschlecht oder das Alter oder eher vertrauliche persönliche Daten, wie das eigene Einkommen oder sexuelle Vorlieben handelt [59]. Die Art der Daten und wie diese individuell bewertet werden, beeinflusst, wie positiv oder negativ ein Individuum einer möglichen Anfrage durch einen Dienstanbieter gegenübersteht.

H_{14}: Die für eine Person subjektive Sensitivität der Daten hat einen signifikant negativen Einfluss auf die Einstellung.

Darüber hinaus stellen manche Datentypen für einige Anwender sogenannte „No-Go"-Daten dar, das heißt, dass diese unabhängig davon, wer diese zu welchem Zweck und unter welchen Umständen anfordert, nicht weitergegeben werden [17]. Die subjektive Sensitivität der Daten hat also einen direkten Einfluss auf das gezeigt Verhalten, unabhängig von anderen Kontextvariablen.

H_{15}: Die für eine Person subjektive Sensitivität der Daten hat einen signifikant negativen Einfluss auf das Privatsphäre-relevante Verhalten, d.h. je höher die Sensitivität, desto weniger Daten werden preisgegeben.

Vertrauen in den Dienst. Vertrauen beschreibt die Überzeugung, dass ein Dienst, bzw. im Allgemeinen der Sozial- oder Geschäftspartner, entsprechend seiner eigenen Aussagen und gültiger Normen handelt. Entsprechend spielen bei der Vertrauensbildung sowohl individuelle Eigenschaften des Vertrauenden sowie desjenigen, dem vertraut wird, eine Rolle. Auf Seiten desjenigen, der vertraut, spielt vor allem die generelle Neigung zu vertrauen eine entscheidende Rolle als Antezedens [60]. Da jedoch jeder Mensch verschiedenen anderen Menschen oder Organisationen unterschiedlich stark vertraut, müssen darüber hinaus aber auch Eigenschaften des jeweiligen Gegenübers signifikant zur Vertrauensbildung beitragen. Mayer et al. [61] schlugen deshalb das latente Konstrukt der Vertrauenswürdigkeit vor, was von anderen Forschern aufgegriffen wurde (z.B. [60], [62]). Die Vertrauenswürdigkeit setzt sich aus den *wahrgenommenen Fähigkeiten*, dem *Wohlwollen* sowie der *Integrität* des Gegenübers zusammen.

Die *wahrgenommenen Fähigkeiten* beziehen sich hierbei auf spezifische Fertigkeiten und Erfahrungen, die derjenige, dem vertraut werden soll, in der relevanten Domäne oder Situation aufweist. So wird beispielsweise von einem Anbieter für E-Mail-Dienste erwartet, dass dieser in der Lage ist, seine Mailserver korrekt zu verwalten und hinreichend abzusichern. Es wird jedoch nicht erwartet, dass derselbe Dienstanbieter verlässliche Tipps für den nächsten Urlaub anbietet. Dieses Konzept der *wahrgenommenen Fähigkeiten* weist hierbei große Parallelen zu Vorschlägen anderer Autoren mit ähnlichem Bedeutungsinhalt, wie beispielsweise Kompetenz [63] oder Expertentum [64], auf.

Das zweite Konstrukt, *Wohlwollen*, bezieht sich auf die wahrgenommene Bereitschaft desjenigen, dem vertraut werden soll, in einer Weise zu handeln, die positiv für den Vertrauenden ist, unabhängig von egozentrischen profitorientierten Motiven. Das heißt derjenige, dem vertraut wird, hat zusätzliche Motivationen, die ihn im Sinne des Vertrauenden handeln lassen, wie z.B. gesetzliche Auflagen, eine soziale Beziehung zum Vertrauenden oder ähnliches.

Die *Integrität* schließlich bezieht sich auf die Wahrnehmung des Vertrauenden, dass der Gegenüber auf Basis von akzeptablen Prinzipien oder Normen handelt. Da die jeweiligen relevanten Fähigkeiten sehr domänenspezifisch sind, ist Vertrauen natürlicherweise auch abhängig vom situativen Kontext.

Generell spielt Vertrauen, also die Überzeugung des Anwenders, dass in seinem Sinne gehandelt wird, also eine Rolle dabei, wie eine Transaktion (von Daten) wahrgenommen wird, d.h. ob diese als gefährlich, ratsam und/oder sinnvoll erachtet wird [65]. Hierbei liegt der Fokus auf der persönlichen Bewertung der spezifischen situativen Risiken.

H_{16}: Das Vertrauen einer Person in den Dienst hat einen signifikant negativen Einfluss auf die spezifischen Privatsphäre-Bedenken.

Zusätzlich zum mildernden Einfluss auf mögliche Privatsphäre-Bedenken schlagen einige Forscher auch einen direkten, die Bedenken umgehenden, Effektpfad für Vertrauen auf das eigentliche Verhalten vor [9], [66].

H_{17}: Das Vertrauen einer Person in den Dienst hat einen signifikant positiven Einfluss auf das Privatsphäre-relevante Verhalten, d.h. je höher das Vertrauen, desto mehr Daten werden preisgegeben.

Subjektive Relevanz der Daten. Dies beschreibt als wie relevant die erfragten Daten durch den Anwender für die Bereitstellung eines Dienstes angesehen werden. Eine der wichtigsten Komponenten eines fairen Informationsaustausches, wie er in der Theorie des sozialen Vertrags (engl.: Social contract theory) von Milne und Gordon sowie Donaldson und Dunfee [67], [68] näher beschrieben wird, ist die Information darüber, wofür bereitgestellte Informationen genutzt werden. Stimmt der für die Informationen angegebene Nutzungszweck plausibel mit dem vom Anwender erwünschten überein, wird der Austausch als fair angesehen und die wahrgenommene Integrität des Dienstanbieters steigt [61]. Entsprechend wird angenommen, dass die subjektive Relevanz der Daten einen signifikanten Einfluss auf die Vertrauensbildung gegenüber dem jeweiligen Dienst hat [69].

H_{18}: Die für eine Person subjektive Relevanz der erhobenen Daten für den zur Verfügung gestellten Dienst hat einen signifikant positiven Einfluss auf das Vertrauen gegenüber dem Dienst.

Subjektive Sicherheit des Dienstes. Dies beschreibt als wie sicher die bereitgestellten Informationen bei dem Dienst angesehen werden, beziehungsweise als wie hoch die Fähigkeiten des Dienstanbieters eingeschätzt werden, die Daten zu schützen. Hierzu gehören sowohl, dass die Informationen nicht durch Dritte manipuliert als auch nicht durch Dritte gesehen werden können. Analog zum angegebenen Nutzungszweck und der damit verbundenen subjektiven Einschätzung der Relevanz der Daten, spielt der beschränkte Informationszugang für dritte Parteien, d.h. die subjektive Sicherheit der durch den Anwender bereitgestellten Daten, eine große Rolle in der Theorie des sozialen Vertrages [67], [68] und damit auch in Bezug auf die Tatsache, ob der Gegenüber als fair und vertrauenswürdig wahrgenommen wird [70], [71].

H_{19}: Die für eine Person subjektive Sicherheit des Dienstes hat einen signifikant positiven Einfluss auf das Vertrauen gegenüber dem Dienst.

Die subjektive Sicherheit der bereitgestellten Informationen, d.h. wie sehr der Anwender davon überzeugt ist, dass Dritte keinen Zugriff auf diese haben, beeinflusst auch die Sorge und das Unwohlsein bei der Nutzung des fraglichen Dienstes [72]. Dies ist besonders der Fall, wenn es sich um Onlinedienste handelt [73].

H_{20}: Die für eine Person subjektive Sicherheit des Dienstes hat einen signifikant negativen Einfluss auf die spezifischen Privatsphäre-Bedenken.

Bereitschaft zu vertrauen. Dies beschreibt die generelle Neigung zu vertrauen. Diese kann als eine relativ zeitstabile Persönlichkeitseigenschaft gesehen werden, die sich in den verschiedensten Situationen relativ konstant auswirkt [61]. Je stärker diese bei einem Anwender ausgeprägt ist, desto

eher glaubt er anderen Menschen oder z.B. auch Aussagen von Unternehmen. Im Kontext der Privatsphäre im digitalen Alltag kommen hierbei vor allem den Datenschutzrichtlinien eine große Bedeutung zu, welche unter anderem Aussagen dazu enthalten, wer auf bereitgestellte Daten überhaupt Zugriff hat und wie diese vor dem Zugriff durch Dritte geschützt sind [71]. Je eher ein Anwender bereit ist, Vertrauen in das Wohlwollen und die Integrität des Dienstes zu setzen, desto größer ist auch sein subjektives Sicherheitsempfinden bei der Bereitstellung von Daten und damit mittelbar auch sein Vertrauen in den Dienst selbst.

H_{21}: Die Bereitschaft einer Person zu vertrauen hat einen signifikant positiven Einfluss auf die subjektive Sicherheit des Dienstes.

Reputation des Dienstes. Die Reputation eines Dienstes stellt die öffentliche, soziale Wahrnehmung desselben dar [74]. Was andere über einen Dienst und dessen Vertrauenswürdigkeit berichten, kann die Wahrnehmung dieses Dienstes durch das Individuum beeinflussen [75]. Eine positive Berichterstattung oder Empfehlungen von anderen als vertrauenswürdig betrachteten Personen haben einen positiven Einfluss auf das Vertrauen, das einem Dienst durch ein Individuum entgegengebracht wird. Verschiedenste Studien konnten dies insbesondere auch im Onlinekontext zeigen [60], [76–79].

H_{22}: Die Reputation des Dienstes hat einen signifikant positiven Einfluss auf das Vertrauen einer Person in den Dienst.

Allgemeine Privatsphäre-Bedenken. Hiermit werden allgemeine, nicht mit einer spezifischen Webseite oder einem bestimmten Dienst verknüpfte Bedenken hinsichtlich der eigenen Privatsphäre beschrieben. Verschiedene Studien zeigten bereits, dass diese allgemeinen Bedenken, wenn sie stark ausgeprägt sind, dazu führen können, dass Anwender sich gegen die Bereitstellung ihrer persönlichen Daten entscheiden [43], [65]. Dennoch zeigten neuere Studien, dass situativen Bedenken mehr Beachtung geschenkt werden sollte, da die Zusammenhänge zwischen allgemeinen Bedenken und dem Verhalten durch die spezifischeren situativen Bedenken mediiert werden [80], [81].

H_{23}: Die allgemeinen Privatsphäre-Bedenken einer Person haben einen signifikant positiven Einfluss auf seine spezifischen Privatsphäre-Bedenken.

Subjektive Kontrollüberzeugung. Die erlebte, d.h. subjektive, Kontrollüberzeugung über das eigene Verhalten ist eine maßgebliche Größe für die Verhaltensbildung und als solche Teil verschiedener grundlegender und allgemeiner Verhaltenstheorien in der Psychologie [36–39], [82], [83]. Sie beschreibt das subjektive Gefühl, eine Handlung erfolgreich ausführen zu können bzw. Einfluss auf oder Kontrolle über das eigene Handeln zu haben. Wird eine Handlung von äußeren Umständen diktiert und steht keine alternative Handlungsweise zur Verfügung, ist folglich die subjektive Kontrollüberzeugung sehr niedrig ausgeprägt. Stehen einem Individuum jedoch verschiedene Handlungspfade offen, die auch verschiedene Erfolgsaussichten haben, so ist die empfundene Kontrollüberzeugung hoch. So kann eine Situation durch ein Individuum beispielsweise als grundsätzlich bedrohlich bewertet werden, solange jedoch erfolgsversprechende Handlungsmöglichkeiten zur Verfügung stehen, die subjektive Kontrollüberzeugung also hoch ist, wird die Situation als Ganzes dennoch als zu bewältigen und damit positiv eingeschätzt. Im digitalen Kontext könnte beispielsweise die Möglichkeit Schadsoftware mittels eines durch das Individuum nutzbaren Virenscanners unschädlich zu machen mögliche Bedenken hinsichtlich des Schadenspotentials abmildern [84], [85].

H_{24}: Die subjektive Kontrollüberzeugung, die eine Person innerhalb einer Situation erlebt, hat einen signifikant negativen Einfluss auf ihre spezifischen Privatsphäre-Bedenken.

Darüber hinaus postuliert die weit verbreitete und etablierte Theorie des geplanten Handelns [36], [86] auch einen direkten Einfluss der subjektiven Kontrollüberzeugung auf das Verhalten als solches, ohne dazwischengeschaltete Faktoren, die als Mediator wirken.

H_{25}: Die subjektive Kontrollüberzeugung, die eine Person innerhalb einer Situation erlebt, hat einen signifikant positiven Einfluss auf ihr Privatsphäre-relevantes Verhalten, d.h. je höher die subjektive Kontrollüberzeugung, desto mehr Daten werden preisgegeben.

Spezifische Privatsphäre-Bedenken. Im Gegensatz zu den allgemeinen beschreiben die spezifischen Privatsphäre-Bedenken Sorgen, die sich direkt auf eine spezifische Situation, im Kontext dieser Arbeit also auf eine Webseite bzw. einen spezifischen Dienst, beziehen. Entsprechend wirken diese spezifischen Bedenken sowohl auf die Bewertung der Situation selbst, d.h. die Einstellung ihr gegenüber, als auch direkt auf das Verhalten [80], [81], [87].

H_{26}: Die spezifischen Privatsphäre-Bedenken, die eine Person innerhalb einer Situation erlebt, haben einen signifikant negativen Einfluss auf ihre Einstellung.

H_{27}: Die spezifischen Privatsphäre-Bedenken, die eine Person innerhalb einer Situation erlebt, haben einen signifikant negativen Einfluss auf ihr Privatsphäre-relevantes Verhalten, d.h. je höher die Bedenken, desto weniger Daten werden preisgegeben.

Subjektive Vorteile. Der Privacy Calculus bietet ein Rahmenwerk zu Erforschung der Bewertung von möglichen Gewinnen und Verlusten und daraus resultierenden Entscheidungen durch Individuen im Kontext von Privatsphäre-relevanten Entscheidungen. Er geht dabei von der Grundannahme aus, dass Menschen stets versuchen, einen optimalen Kompromiss aus möglichen Risiken und Gewinnen zu erreichen [43]. Von dieser Grundannahme des Homo Oeconomicus [88] haben sich verschiedene Theorien zur Entscheidungsfindung von Menschen abgeleitet, die sich mit der Abwägung zwischen potentiellen Gewinnen, oder Vorteilen, und möglichen Risiken oder Verlusten beschäftigen (z.B. [44], [45]), die sich letztlich auch das Privacy Calculus Rahmenwerk einordnen lassen. Die Nützlichkeits-Maximierungs-Theorie (engl. utility maximization theory) [45] postuliert dabei, dass die Differenz zwischen möglichen Gewinnen und potentiellen Verlusten, also die Nützlichkeit eines Verhaltens, stets in Richtung der Gewinne optimiert wird.

H_{28}: Die subjektiven Vorteile für eine Person haben einen signifikant positiven Einfluss auf ihr Privatsphäre-relevantes Verhalten, d.h. je höher die Vorteile, desto mehr Daten werden preisgegeben.

Ein anderes Beispiel ist die Valenz-Instrumentalitäts-Erwartungs-Theorie (engl. expectancy theory of motivation) [69], [89], welche die Erwünschtheit der möglichen Konsequenzen mit der Handlungsabsicht verknüpft. Diese Verknüpfung wird durch drei verschiedene kognitive Prozesse erreicht, einer davon ist die Valenzbewertung, d.h. der positive (oder negative) Wert, den ein Individuum einem bestimmten Ergebnis einer Handlung zuschreibt. Dieser Prozess ist äquivalent zur Einstellung gegenüber einem Verhalten oder einem Dienst (vgl. folgender Absatz).

H_{29}: Die subjektiven Vorteile für eine Person haben einen signifikant positiven Einfluss auf ihre Einstellung.

Einstellung gegenüber dem Verhalten. Die Theorie des geplanten Verhaltens [36] beschreibt verschiedene kognitive Prozesse, die zur Verhaltensbildung beitragen, dem Verhalten selbst also vorausgehen. Einer dieser Prozesse bildet die Einstellung gegenüber einem Verhalten (z.B. einen Dienst zu nutzen) aus Kombination der Stärken verschiedener Grundüberzeugungen und den zugehörigen positiven oder negativen Bewertungen. Die Einstellung bildet also eine generelle Bewertung eines Verhaltens in positiver oder negativer Richtung. Sie begünstigt im positiven Fall also die Verhaltensäußerung und hemmt sie im negativen.

H_{30}: Die Einstellung einer Peron hat einen signifikant positiven Einfluss auf ihr Privatsphäre-relevantes Verhalten, d.h. je positiver die Einstellung, desto mehr Daten werden preisgegeben.

Zusammenfassung. Insgesamt enthält das integrative Forschungsmodell 20 Faktoren sowie 30 Hypothesen, d.h. postulierte Wirkzusammenhänge. Die Faktoren lassen sich in vier verschiedene Kategorien einteilen, wie sie auch in Abbildung 17 farblich hervorgehoben sind.

In Rot die Zwischensubjekt-Erfahrungsunterschiede, d.h. jene Faktoren, die die unterschiedlichen Erfahrungsniveaus verschiedener Individuen erfassen. Darunter fallen beispielsweise frühere positive oder negative Erfahrungen mit Onlineversandhäusern. In Gelb die Zwischensubjekt-Kognitionsunterschiede, also jene Faktoren, die allgemeine kognitive Vorgänge beschreiben, die zwischen verschiedenen Individuen unterschiedlich sind. Hierzu gehört beispielsweise die

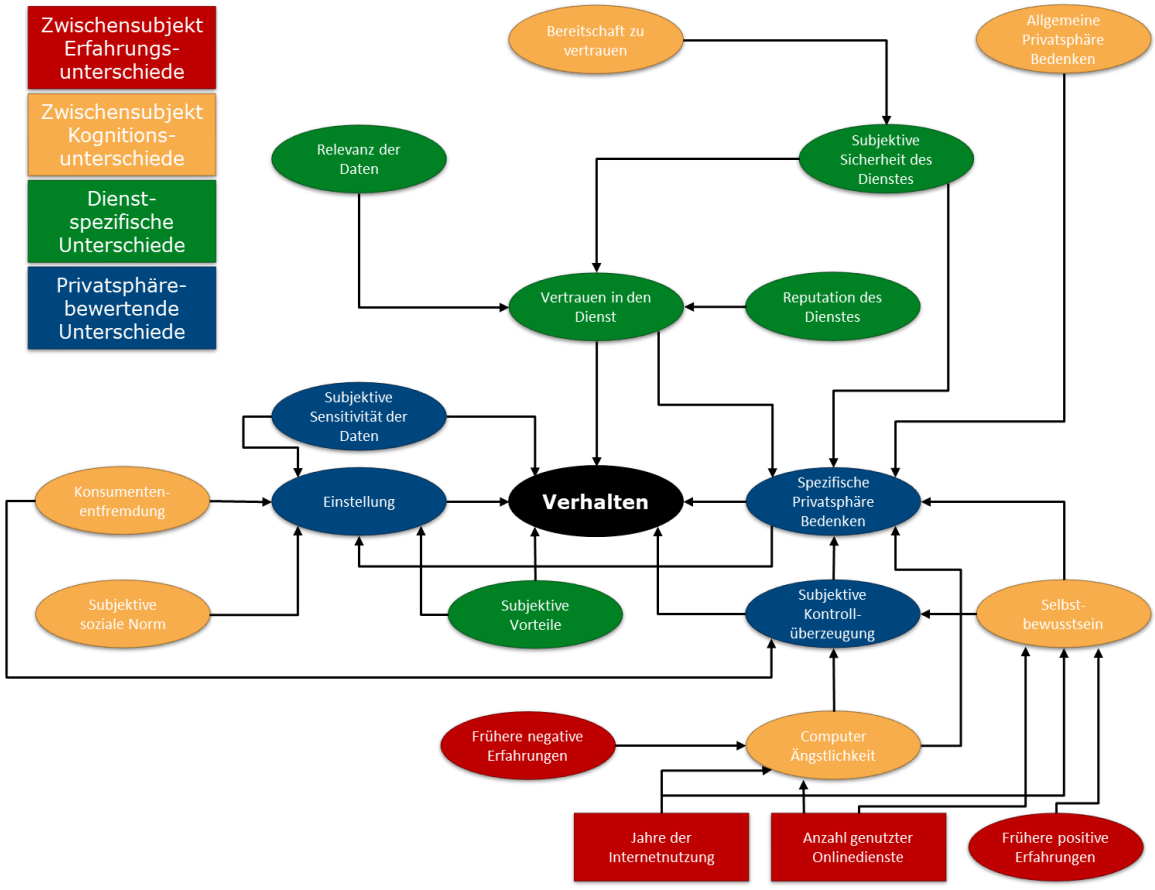

Abbildung 17. Überblick über das Forschungsmodell

unterschiedliche Wahrnehmung der sozialen Norm oder auch die individuelle Bereitschaft, anderen zu vertrauen. In Grün sind die dienstspezifischen Unterschiede eingetragen, also jene Faktoren, die direkte Unterschiede zwischen verschiedenen Diensten betreffen. Hierzu gehören beispielsweise die Reputation oder auch die individuell gebotenen Vorteile eines Dienstes. Schließlich in Blau die direkt Privatsphäre-bewertenden Unterschiede, d.h. jene Faktoren die mit der direkten Bewertung der Privatsphäre-Situation zu tun haben. Hierzu gehört beispielsweise die subjektive Kontrollüberzeugung, d.h. wie sehr ist ein Individuum überzeugt Einfluss auf die aktuelle Situation ausüben zu können, oder auch als wie sensitiv angefragte Daten empfunden werden.

4.2.2. Bewertung des Forschungsmodells auf Basis der früheren empirischen Ergebnisse

Die in Kapitel 2 und 3 gewonnenen Erkenntnisse liefern Hinweise darauf, welche Informationen für die Entscheidung für oder gegen eine Applikation sinnvoll und nützlich sind. Ein Vergleich mit den entscheidungsbildenden Faktoren aus der Literatur (vgl. Kapitel 4.2.1) erscheint insofern nützlich, als dass eventuell vorhandene Lücken identifiziert werden können, welche eine gezieltere Recherche zur Folge hätten.

Die in Kapitel 2.1.3 abgeleiteten Heuristiken gliedern sich in insgesamt vier Teilaspekte, berechtigungsbasierte, entwicklerorientierte, sozialbasierte sowie vermeidungsbasierte Heuristiken. Diese vier Kategorien und die zugehörigen einzelnen Heuristiken werden im Folgenden in das in Kapitel 4.2.1 postulierte Forschungsmodell eingeordnet.

4.2.2.1. Berechtigungsbasierte Heuristiken

In Bezug auf die Berechtigungen einer Applikation gilt es zu bewerten, ob diese sowohl angemessen für die gebotene Funktionalität als auch akzeptabel für einen selbst als Anwender sind. Eine Bewertung der Angemessenheit der Berechtigungen (d.h. der genutzten bzw. abgefragten Daten) gemessen an der Funktionalität ist letztlich eine Prüfung der Relevanz der Daten. Es gilt zu abzugleichen, ob die (persönlichen) Daten, die ein Dienstanbieter (bzw. eine Applikation) nutzen möchte, relevant für die gebotene Funktionalität sind. Dies entspricht Hypothese 18. Die Frage, ob die genutzten Daten auch akzeptabel für den individuellen Anwender sind, spiegelt sich in der Bewertung der spezifischen Privatsphäre-Bedenken und deren Wechselwirkung mit dem Verhalten wider. Dies entspricht Hypothese 27.

4.2.2.2. Entwicklerorientierte Heuristiken

Die Heuristiken, die sich direkt auf den Entwickler beziehen, beinhalten eine Prüfung der Reputation des selbigen, der Webseite, des Updateverhaltens sowie die Betrachtung anderer Applikationen oder Dienste, die vom gleichen Entwickler angeboten werden. Die Reputation selbst ist direkt im Verhaltensmodell in Hypothese 22 enthalten. Auf der Entwicklerhomepage finden sich ggf. objektive Informationen, wie z.B. Datenschutzbestimmungen, aber sie trägt auch zum subjektiven Eindruck bei, beispielsweise in Bezug auf die Sorgfalt des Entwicklers. Insbesondere die Bewertung der Datenschutzbestimmungen findet sich im Forschungsmodell in der Vertrauensbildung, d.h. den Hypothesen 18 und 19, wieder. Die Einschätzung über das Updateverhalten wurde vor allem im Kontext der Schließung möglicher Sicherheitslücken genannt, also der Einschätzung der subjektiven Sicherheit. Diese findet sich ebenfalls direkt im Forschungsmodell in den Hypothesen 19 und 20. Die

Bewertung anderer Angebote des gleichen Entwicklers kann entweder frühere eigene Erfahrungen adressieren (Hypothesen 5 und 6), die Reputation an sich oder beispielsweise auch soziales Feedback in Form von Reviews und Bewertungen anderer Anwender (Hypothese 13) erfassen.

4.2.2.3. Sozialbasierte Heuristiken

Die dritte Kategorie beinhaltet Heuristiken zu sozialen Informationen, d.h. die Prüfung der Nutzerbasis in Form der Downloadzahlen, die Empfehlungen von Freunden oder vertrauenswürdigen Personen, Reviews von anderen Nutzern, Bewertungen sowie ggf. eine direkte Kontaktaufnahme mit dem Entwickler. Die meisten dieser Informationen finden sich in der subjektiven sozialen Norm (Hypothese 13) wieder. Darüber hinaus können Reviews beispielsweise auch Informationen zu möglichen Risiken oder Bedenken anderer Anwender enthalten und insofern direkt spezifische Privatsphäre-Bedenken adressieren. Sie können aber auch, ebenso wie ein positiver Kontakt mit dem Entwickler selbst, der z.B. ausführlich bei Fragen oder Problemen hilft, direkt das Vertrauen in den Dienst bzw. den Entwickler stärken (Hypothese 18, 19 sowie 22).

4.2.2.4. Vermeidungsbasierte Heuristiken

Die letzte Kategorie schließlich umfasst Vermeidungsstrategien, mit denen sich Probleme oder Bedenken lösen lassen, wie beispielsweise die minimale Installation von Applikationen oder die Beschränkung auf Applikationen, die genau die Funktionalitäten bietet, die benötigt werden. Aber auch die Vermeidung der Speicherung sensitiver Daten auf dem Smartphone selbst. Die meisten dieser Heuristiken beziehen sich bereits direkt auf spezifisches Verhalten, welches durch das Modell erklärt werden soll und somit nicht direkter Teil der Erklärung, d.h. der Faktoren ist. Die minimalisierte Installation von Applikationen beziehungsweise die Nutzung von funktional möglichst passenden Applikationen als Verhaltensalternativen kann jedoch der Wechselwirkung zwischen subjektiver Kontrolle und spezifischen Privatsphäre-Bedenken zugeordnet werden (Hypothese 24).

Die Betrachtung der verschiedenen Heuristiken im Kontext des auf Basis der Literatur formulierten integrativen Verhaltensmodells brachte keine a priori erkennbaren Erklärungslücken zum Vorschein. Das Modell bietet ergänzend eine strukturiertere Übersicht über die verschiedenen Faktoren, zusätzlich zu der direkten und spezifisch handlungsorientierten Sammlung von Heuristiken für die Applikationsauswahl. Im folgenden Kapitel wird detailliert auf die Studie zur Überprüfung des formulierten Forschungsmodells eingegangen.

4.3. Überprüfung des integrativen Verhaltensmodells

Im folgenden Kapitel wird die durchgeführte Studie zur Überprüfung des postulierten Modells detailliert vorgestellt. Hierfür wird zunächst auf Studiendesign und -ablauf eingegangen. Im darauffolgenden Unterkapitel wird auf die zur Überprüfung des Modells erhobene Stichprobe eingegangen, gefolgt von einer Auflistung und Beschreibung der verwendeten Messinstrumente. Danach werden die Ergebnisse der Überprüfung des Messmodells vorgestellt, um in Anschluss daran auf die Ergebnisse der Strukturgleichungsmodellierung einzugehen.

4.3.1. Studienablauf

Die Studie gliedert sich insgesamt in vier Phasen und wurde bei SoSciSurvey[34] in Deutschland gehostet.

Phase 0: Begrüßung und Einführung. Die Studie startete mit einer kurzen Beschreibung des vorgeblichen Themas der aktuellen Studie, der voraussichtliche Dauer sowie einer Instruktion, wie nach der Teilnahme die Vergütung erfolgt. Außerdem wurde die für die Studie verantwortliche Institution, d.h. in diesem Fall die Technische Universität Darmstadt, benannt. Als Thema der Studie wurde generisch „Entscheidungsfindung" („decision making") angegeben.

Phase 1: Verhaltensmessung. Zu Beginn dieser Phase stand ein kurzer Instruktionstext. Dieser wies darauf hin, dass nun einige persönliche Fragen gestellt werden, jedoch nur solche, die für die Forschung benötigt werden. Darüber hinaus erwähnte er, dass jede Frage freiwillig ist und jede davon mittels „das möchte ich nicht sagen" („I prefer not to say") übersprungen werden kann. Danach folgten die insgesamt 77 Verhaltensitems (vgl. Tabelle 10 im Anhang A3 ab Seite 90).

Phase 2: Faktoren der Verhaltensbildung. Zu Beginn dieser Phase, nach Abschluss der Verhaltensmessung, wurde den Teilnehmern der wahre Hintergrund der Studie mitgeteilt. Der Erklärungstext wies darauf hin, dass sich die Studie eigentlich mit Privatsphäre-relevanten Entscheidungen beschäftigt. Zusätzlich wurde darauf hingewiesen, dass die Antworten aus dem ersten Teil zum Schutz der Privatsphäre der Teilnehmer nicht gespeichert werden. Es wurde einzig gespeichert, ob die Teilnehmer eine Antwort gegeben oder die Frage übersprungen haben. Der eigentliche Inhalt der Antwort wurde automatisiert gelöscht. Für die folgenden Fragen zu den Faktoren der Verhaltensbildung wurden die Teilnehmer zum Schluss des Textes aufgefordert, zu versuchen, sich daran zu erinnern, wie sie sich beim Ausfüllen des ersten Teils gefühlt haben und entsprechend zu antworten. Im Folgenden beantworteten die Teilnehmer die Fragen, welche zur Messung der verschiedenen in den Hypothesen (vgl. Kapitel 4.2.1 ab Seite 50) genannten Konstrukten dienten. Diese sind in Tabelle 6 zusammengefasst.

Phase 3: Demographie und Verabschiedung. Zum Abschluss wurden die Teilnehmer nach allgemeinen demographischen Angaben (Alter, Geschlecht, Bildung) gefragt. Diese wurden zwar bereits in Phase 1 der Studie abgefragt, dort jedoch noch unter Angabe eines falschen Zweckes. Da diese Angaben entsprechend der Aufklärung zu Beginn von Phase 2 gelöscht wurden, wurde an dieser Stelle erneut danach gefragt. Danach wurde der für den Erhalt der Vergütung notwendige Teilnahmecode angezeigt und der Teilnehmer bzw. die Teilnehmerin verabschiedet.

4.3.2. Stichprobe

Insgesamt nahmen 348 Probanden an der Umfrage teil. 23 davon gehörten zum Vortest, 35 mussten auf Grund von eindeutig falschem Antwortverhalten (z.B. stets rechts- bzw. linksseitige Antworten trotz invertierter Items, vorzeitiger Abbruch oder eine zu kurze Bearbeitungszeit) ausgeschlossen werden. Somit wurden final insgesamt Antworten von 290 Befragten ausgewertet.

Die Teilnehmer wurden mittels Amazon Mechanical Turk rekrutiert, eine kostenpflichtige Plattform, mit der schnell große Stichproben von Teilnehmern gezogen werden können und die in den letzten Jahren sehr populär für größere Onlinestudien wurde [90]. Die Teilnehmer wurden auf

[34] www.soscisurvey.de

nordamerikanische IP Adressen beschränkt. Als zusätzliche Einschränkung wurden nur Teilnehmer zugelassen, die eine Annahmequote von 90% oder mehr auf der Plattform aufwiesen. Diese Einschränkungen orientieren sich an in der Forschung üblichen Maßstäben für Mechanical Turk (z.B. [30]). Für eine erfolgreiche Teilnahme erhielt jeder Teilnehmer 2$. Im Durchschnitt benötigten die Teilnehmer 889,4 Sekunden (SD = 320,4s) zum Ausfüllen der Studie.

Die Teilnehmer waren im Durchschnitt 34,8 Jahre alt (SD = 10,4 Jahre). Insgesamt nahmen 151 Männer und 138 Frauen teil. Nur ein Teilnehmer wählte die Option „Sonstiges" bei Geschlecht. Über zumindest einen Highschool-Abschluss verfügten 70 (24,1%) Teilnehmer, 155 (53,4%) verfügten über einen College-Abschluss und 64 (22,1%) über einen Universitätsabschluss. Ein Teilnehmer macht dazu keine Angaben.

4.3.3. Messmethoden

Die Messinstrumente für die latenten Konstrukte Verhalten, subjektive soziale Norm sowie für die subjektiven Vorteile, die durch die Nutzung eines Dienstes entstehen, sind die einzigen, die für diese Studie selbst konstruiert wurden. Alle anderen wurden aus bestehender englischsprachiger Literatur übernommen und zeigten dort jeweils angemessene psychometrische Eigenschaften. Da die Stichprobe selbst englischsprachig war, entfiel die Notwendigkeit einer Übersetzung, welche die psychometrischen Eigenschaften der Skalen gefährdet hätte. Tabelle 6 fasst die einzelnen Messinstrumente für jedes latente und manifeste Konstrukt zusammen. Soweit nicht anders direkt beim Konstrukt angegeben, handelt es sich um siebenstufige Likert-Skalen.

Die Items, die zur Messung des Verhaltens verwendet wurden, wurden in mehreren Runden iterativ zusammengestellt. Als erster Startpunkt wurde die Sammlung von Norberg et al. [9] genutzt. Diese wurde jedoch deutlich erweitert und modifiziert, um ein breites Spektrum abzudecken. Ziel hierbei war es, möglichst invasive Fragen zu generieren, die von einem nennenswerten Anteil der Stichprobe (>10%) nicht beantwortet werden, sodass die Daten hinreichend Varianz aufweisen, um eine statistische Auswertung zu ermöglichen.

Es wurden insgesamt 77 Fragen aus verschiedenen Bereichen zusammengestellt. Insgesamt 49 davon stellten Fragen nach Fakten aus dem Leben der Teilnehmer dar, welche mit ja oder nein bzw. einem offenen Format zu beantworten waren. Die restlichen 28 waren Fragen nach persönlichen Meinungen mit einem siebenstufigen Likert-Skalen Format. Die Fragen stammen aus insgesamt sechs verschiedenen Bereichen:

1. Fakten (z.B. Einkommen, absolvierte Praktika in der Vergangenheit)
2. Politisches (z.B. Teilnahme an der letzten Wahl, Meinung zu Donald Trump als Präsident)
3. Gesundheit (z.B. Allergien, frühere Operationen, Krankheiten in der Familie)
4. Religion (z.B. eigene Konfession, Meinung zur katholischen Kirche)
5. Intime Beziehungen (z.B. Anzahl Sexualpartner, liebste Sexstellung)
6. Ordnungswidrigkeiten (z.B. Fahrerflucht nach „Parkplatzunfall", Ladendiebstahl)

Alle Verhaltensfragen sind im Anhang A3 ab Seite 90 in Tabelle 10 enthalten. Die zugehörigen Häufigkeiten, wie oft jede Frage durch die Teilnehmer beantwortet wurde, sind ebenfalls dort zu finden.

Die Items zur Erfassung der subjektiven sozialen Norm wurden den Empfehlungen von Ajzen [36] entsprechend konstruiert, wohingegen die Items für die Erfassung der subjektiven Vorteile auf den Erkenntnissen einer bisher unveröffentlichten Onlinestudie beruhen, welche während des zweiten

Workshops des MoPPa-Projektes[35] in Darmstadt am 24.04.2017 vorgestellt wurde [91]. In der Onlinestudie wurden die Teilnehmer u.a. dazu befragt, welche Ziele und Absichten sie bei der Nutzung verschiedener Produkte oder Dienste verfolgen. Bei einer der abgefragten Dienste-Kategorien handelte es sich um die Teilnahme an Forschungsstudien bzw. Marktforschungsstudien. Insgesamt nahmen an der Studie 231 Teilnehmer teil. Die Antworten aus diesem Bereich wurden genutzt, um die Items zu formulieren, da es sich bei der aktuellen Studie zur Überprüfung des integrativen Verhaltensmodells letztlich in der Wahrnehmung der Teilnehmer um eine Forschungsstudie handelte (vgl. Kapitel 4.3.1 ab Seite 60).

Die beiden manifesten Variablen Jahre der Internetnutzung sowie Anzahl der genutzten Onlinedienste wurden direkt als Frage mit offenem Antwortformat mit Beschränkung auf ganze Zahlen erhoben. Demographische Informationen (Alter, Geschlecht, Bildung) wurden jeweils als einzelne Items erhoben.

Tabelle 6. Übersicht über die Items aller latenten und manifesten Konstrukte der Studie inklusive der jeweiligen Mittelwerte (M), Standardabweichung (SD) und Faktorladungen (FL); invertierte Items sind mit (R) gekennzeichnet und entsprechende Mittelwerte transformiert

Konstrukt bzw. Item	M	SD	FL
Frühere Erfahrungen mit Onlinediensten – negativ [81]			
I have had bad experiences with regard to my online privacy before.	3,01	1,86	0,91
I was a victim of online privacy invasion.	2,72	1,88	0,93
I believe that my online privacy was invaded in by other people or organizations.	3,02	1,93	0,90
Frühere Erfahrungen mit Onlinediensten – positiv [70]			
The extent of usefulness of survey sites for me in the past has been very high.	4,97	1,51	-0,64
I often have benefited from participating in surveys.	5,66	1,36	-0,85
My positive encounters with survey sites has been numerous.	5,47	1,43	-0,84
The extent of usefulness of Amazon Mechanical Turk for me in the past has been very high.	5,86	1,31	-0,88
I often have benefited from working at Amazon Mechanical Turk.	6,08	1,15	-0,85
My positive encounters with Amazon Mechanical Turk has been numerous	5,86	1,31	-0,81
Jahre der Internetnutzung			
How many years have you been using the Internet?	18,13	4,49	-
Anzahl genutzter Onlinedienste			
How many different online services approximately do you use on a regular basis?	9,27	11,01	-
Computerängstlichkeit [53]			
Computers are a real threat to privacy in this country.	4,73	1,66	-0,52
Sometimes I'm afraid I'll damage a computer if I use it.	1,86	1,43	-0,55

[35] http://www.arbing.psychologie.tu-darmstadt.de/projekte_6/projects_moppa/projects_moppa.de.jsp ; letzter Abruf 04.10.2017

Konstrukt bzw. Item	M	SD	FL
I am anxious and concerned about the pace of automation in the world.	3,37	1,93	-0,86
I am sometimes frustrated by increasing automation in my home.	2,68	1,73	-0,83
Selbstbewusstsein [53]			
I feel that I have a number of good qualities.	5,86	1,40	0,87
All in all, I am inclined to feel that I am a failure. (R)	5,71*	1,75	0,87
I am able to do things as well as most other people.	5,72	1,48	0,91
I take a positive attitude toward myself.	5,47	1,70	0,93
On the whole, I am satisfied with myself.	5,31	1,73	0,89
Konsumenten Entfremdung [53]			
It is not unusual to find out that businesses lied to the public.	5,71	1,41	0,64
Stores do not care why people buy their products just as long as they make a profit.	5,08	1,68	0,72
Business' prime objective is to make money rather than to satisfy the consumer.	5,53	1,33	0,82
It is difficult to identify with business practices today.	4,90	1,60	0,76
Unethical practices are widespread throughout business.	5,47	1,49	0,81
Subjektive soziale Norm (selbst konstruiert auf Basis von [36]*)*			
People who influence my behavior think that I should participate in surveys via Amazon Mechanical Turk.	3,27	1,82	0,96
People who are important to me think that I should participate in surveys via Amazon Mechanical Turk.	3,50	1,90	0,96
Subjektive Sensitivität der Daten [70] *– siebenstufige Skala; 0 = not sensitive at all und 7 = very sensitive*			
If disclosed online, how would you personally assess information about …			
… your personal relationships?	4,42	1,89	0,84
… factual information about you (e.g. your monthly income)?	4,87	1,80	0,84
… your health status or history?	4,74	1,93	0,86
Bereitschaft zu vertrauen [92]			
I generally trust other people.	4,59	1,58	0,94
I tend to count upon other people.	4,19	1,69	0,89
I generally have faith in humanity.	4,39	1,68	0,85
Subjektive Sicherheit des Dienstes [93]			
I believed the information I provided in part one will be manipulated by inappropriate parties. (R)	5,46*	1,51	0,82
I believed inappropriate parties may deliberately view the information I provide in part one this survey. (R)	5,22*	1,56	0,76

Konstrukt bzw. Item	M	SD	FL
Relevanz der Daten [94]			
Information gathered in part one of the survey seemed relevant for the purpose of the survey at first stated.	5,03	1,62	0,80
Questions in the first part appeared to have a bearing upon the purpose of the survey study stated on the starting page.	4,81	1,67	0,89
Information collected in the first part of the survey looked appropriate for the survey.	4,98	1,65	0,83
Reputation des Dienstes [81]			
I thought this survey site has a good reputation.	5,14	1,34	0,86
I thought this survey site has a good reputation compared to other rival websites.	4,96	1,39	0,85
I thought this survey site has a reputation for being respectful to its participants.	5,11	1,38	0,83
Vertrauen in den Dienst [70] – *fünfstufiges semantisches Differential*			
I believe that this survey site …			
… is honest at all vs. is very honest.	3,92	0,83	0,73
… cares about its own interests only vs. cares about its participants all the time.	3,69	0,94	0,87
… is opportunistic vs. is dependable.	3,86	0,95	0,87
Allgemeine Privatsphäre Bedenken [65]			
Compared to others, I am more sensitive about the way online companies handle my personal information.	3,71	1,81	0,77
To me, it is the most important thing to keep my privacy intact from online companies.	4,50	1,73	0,81
I am concerned about threats to my personal privacy today.	4,66	1,79	0,80
Subjektive Kontrolle [95]			
I believe I have control over who can get access to my personal information collected in this survey.	3,48	2,00	0,89
I believe I have control over how my personal information is used in this survey.	3,36	2,02	0,91
I believe I can control my personal information provided in this survey.	4,09	2,20	0,82
Spezifische Privatsphäre Bedenken [81]			
I am concerned that this website is collecting too much information about me.	3,44	1,95	0,63
I am concerned about my privacy when browsing this website.	3,46	1,78	0,59
My personal information could be misused when transacting with this website.	4,25	1,84	0,86
My personal information could be accessed by unknown parties when transacting with this website.	4,24	1,81	0,88

Konstrukt bzw. Item	M	SD	FL
Subjektive Vorteile (selbst konstruiert auf Basis von [91]*)*			
Providing my personal information in part one of the survey seemed beneficial to me since I get money. (D)	5,27	1,49	<0,4
Providing my personal information in part one of the survey seemed beneficial to me since I could help the researchers.	5,28	1,59	0,71
Providing my personal information in part one of the survey seemed beneficial to me since I'm interested in the topic.	4,26	1,81	0,88
Providing my personal information in part one of the survey seemed beneficial to me since I had fun.	3,76	1,81	0,84
Einstellung gegenüber dem Verhalten [96] *– 10 Punkt semantisches Differential*			
I think that giving factual information (e.g. my income) about me to others via the internet is:			
Not useful vs. very useful	6,16	2,40	0,57
Disadvantageous vs. advantageous	5,79	2,30	0,59
Very dangerous vs. not dangerous	6,02	2,41	0,87
Careless vs. not careless	5,90	2,37	0,89
Very bad vs. very good	5,68	1,86	0,82
I think that giving information about my relationships to others via the internet is:			
Not useful vs. very useful	5,89	2,59	0,80
Disadvantageous vs. advantageous	5,89	2,28	0,90
Very dangerous vs. not dangerous	6,61	2,49	0,81
Careless vs. not careless	6,39	2,45	0,85
Very bad vs. very good	6,03	2,09	0,90
I think that giving information about my health status or history to others via the internet is:			
Not useful vs. very useful	5,97	2,65	0,78
Disadvantageous vs. advantageous	5,76	2,59	0,88
Very dangerous vs. not dangerous	5,91	2,68	0,93
Careless vs. not careless	5,74	2,69	0,94
Very bad vs. very good	5,68	2,42	0,93
Verhalten (selbst konstruiert) – angeben = 1; keine Antwort = 0			
– Beziehung			
How often do you masturbate per week?	0,80	0,40	0,82
How often do you have oral sex per week?	0,83	0,37	0,81
How many different sexual partners did you had?	0,86	0,35	0,80
Which are your most favorite sexual positions?	0,64	0,48	0,70
At what age did you have sex for the first time?	0,88	0,33	0,69
– demographische Fakten			
What internships did you do in your life?	0,84	0,37	0,86
What was your school final grade point average?	0,88	0,33	0,81
What extracurricular activities did you do in school?	0,85	0,36	0,84

Konstrukt bzw. Item	M	SD	FL
– *Gesundheit*			
Do one or more members of your family suffer from any other disease (e.g. cancer or Alzheimer)?	0,81	0,39	0,70
Einführende Instruktion für alle Fragen außer den Verhaltensfragen:			
Please assess to which extent you agree with the following statements while you think about the feelings you had during the first part of the study, i.e. before you know, that we won't analyze your actual personal information.			

M – Mittelwert; SD – Standardabweichung; FL – Faktorladung
(R) Invertierte Formulierung; *Invertierter Mittelwert transformiert auf Basis der 7-Punkt-Likert-Skala
(D) Auf Grund ungenügender psychometrischer Qualität aus Skala entfernt

Die Messinstrumente wurden in einer Vorstudie getestet. Daran nahmen insgesamt 23 Probanden teil. Nach dieser Vorstudie wurden noch sechs weitere Verhaltensitems hinzugefügt. Das sonstige Messinventar wurde unverändert beibehalten.

4.3.4. Ergebnisse

Alle Messungen wurden zunächst hinsichtlich ihrer Reliabilität und Validität untersucht. Hierfür wurden Cronbachs Alpha und faktorenanalytische Methoden genutzt um die Reliabilität, Konvergenzvalidität[36] und Diskriminanzvalidität[37] zu untersuchen. Die zugehörigen Ergebnisse werden im Folgenden beschrieben. Danach folgen die Ergebnisse der Modellierung mittels eines Strukturgleichungsmodells.

Überprüfung des Messmodells. Die Faktorladungen jedes Items für jedes latente Konstrukt finden sich in Tabelle 6 in der letzten Spalte. Die Werte für Cronbachs Alpha, Faktorenreliabilität und die durchschnittliche extrahierte Varianz sowie deren Quadratwurzel für jedes Konstrukt finden sich in Tabelle 7. Alle Reliabilitätskennwerte liegen über der Schwelle 0,7, sodass von einer hinreichenden Reliabilität ausgegangen werden kann [81], [97]. Die Quadratwurzel der durchschnittlich extrahierten Varianz ist für jedes Konstrukt größer als die Korrelation (vgl. Tabelle 9 in Anhang A3 ab Seite 89) mit anderen Konstrukten. Alle extrahierten Varianzen sind mindestens auf dem Niveau des Mindestlevels von 0,5 [97] und alle Faktorladungen (vgl. Tabelle 6) liegen über dem Grenzwert von 0,5, sodass die verwendeten Konstrukte eine akzeptable Konvergenzvalidität aufweisen. Die Diskriminanzvalidität kann anhand der Faktorladungen und Kreuzladungen zu anderen Faktoren ermessen werden. Alle Faktorladungen für alle Konstrukte liegen über dem Grenzwert von 0,5 ohne signifikante Kreuzladungen, sodass von einer hinreichenden Diskriminanzvalidität ausgegangen werden kann.

Überprüfung des Forschungsmodells. Zur Überprüfung des Forschungsmodells wurde ein Strukturgleichungsmodell mittels der AMOS Software[38] (Analysis of moment structure) von IBM modelliert und berechnet. Der Datensatz erfüllte alle Anforderungen an diese Methode, d.h. intervallskalierte oder dichotome Daten, Normalverteilung, keine Multikollinearität, ein überidentifiziertes Modell und eine hinreichende Stichprobengröße.

[36] Konvergenzvalidität liegt dann vor, wenn verschiedene Messungen desselben Konstrukts übereinstimmen
[37] Diskriminanzvalidität liegt dann vor, wenn sich Messungen verschiedener Konstrukte unterscheiden
[38] http://www.spss.com/amos/

Tabelle 7. Überblick über die psychometrischen Kennwerte jedes Konstruktes

Konstrukt	Cronbachs Alpha	Faktoren-reliabilität*	Extrahierte Varianz	Wurzel der extrahierten Varianz	Faktor-nummer
Einstellung	0,95	0,97	0,70	0,84	1
Selbstbewusstsein	0,94	0,95	0,80	0,90	2
Frühere negative Erfahrungen	0,91	0,94	0,83	0,91	3
Konsumenten Entfremdung	0,81	0,87	0,56	0,75	4
Verhalten	0,82	0,93	0,61	0,78	5
Reputation des Dienstes	0,91	0,88	0,72	0,85	6
Subjektive Kontrolle	0,87	0,91	0,76	0,87	7
Frühere positive Erfahrungen	0,90	0,92	0,67	0,82	8
Subjektive Soziale Norm	0,93	0,96	0,92	0,96	9
Computerängstlichkeit	0,71	0,79	0,50	0,71	10
Wahrgenommene Sicherheit	0,70	0,77	0,63	0,79	11
Bereitschaft zu vertrauen	0,88	0,92	0,80	0,89	12
Allgemeine Privatsphäre-Bedenken	0,80	0,84	0,63	0,79	13
Subjektive Vorteile	0,75	0,85	0,66	0,81	14
Spezifische Privatsphäre-Bedenken	0,85	0,84	0,57	0,75	15
Vertrauen in den Dienst	0,87	0,86	0,68	0,82	16
Relevanz der Daten	0,86	0,88	0,71	0,84	17
Subjektive Sensitivität der Daten	0,80	0,88	0,72	0,85	18
Anzahl der genutzten Dienste		(manifeste Variable)			19
Jahre der Internetnutzung		(manifeste Variable)			20

*auch Kongenerische Reliabilität bzw. „composite reliability" (engl.)

Abbildung 18 zeigt das Forschungsmodell inklusive der standardisierten Pfadkoeffizienten sowie der Fit-Indizes. Die Fit Indizes zeigen eine gute bis sehr gute Passung zwischen Modell und Datensatz. Wie in der Literatur empfohlen, sollte stets mehr als ein Index betrachtet werden [98], [99]. Da der χ^2 Test sehr anfällig für die bei SEM Studien erforderlichen großen Stichproben ist [98] werden zusätzlich RMSEA [100] und SRMR [101], wie von [99] empfohlen, betrachtet. Beide liegen unterhalb der empfohlenen Grenzen (RMSEA < 0,6; SRMR < 0,08).

Es können nicht alle Hypothesen bestätigt werden. Neun der insgesamt dreißig Versuchshypothesen müssen verworfen werden, eine zeigt signifikante Zusammenhänge, jedoch mit zur Hypothese invertierter Richtung, die restlichen zwanzig Hypothesen können bestätigt werden. Tabelle 8 gibt eine Übersicht über die geprüften Hypothesen, die zugehörigen standardisierten Regressionsgewichte sowie die zugehörigen p-Werte.

4.4. Diskussion und Interpretation der Ergebnisse

Das integrative Verhaltensmodell bietet insgesamt zufriedenstellende Fit-Werte, auch wenn nicht alle Hypothesen bestätigt werden können. So erweisen sich insgesamt drei der sechs postulierten direkten Effekte auf das Privatsphäre-relevante Verhalten im integrativen Verhaltensmodell als signifikant, wohingegen die anderen keine oder nur indirekte Effekte auf das Verhalten haben. Als stärkster direkter Effekt auf das Verhalten manifestiert sich die subjektive Sensitivität der Daten, danach gleichstark, jedoch entgegengesetzt gerichtet die spezifischen Privatsphäre-bedenken sowie die subjektiven Vorteile.

Entgegen den auf die Literatur gestützten Erwartungen zeigt sich kein statistisch signifikanter Effekt der Einstellung auf das gezeigte Verhalten. Jedoch offenbaren sich signifikante Zusammenhänge mit drei anderen Faktoren, die wiederrum direkte signifikante Effekte auf das Verhalten haben: Die spezifischen Privatsphäre-Bedenken, die subjektiven Vorteile sowie die subjektive Sensitivität der Daten. Die Einstellung beinhaltet also jeweils gemeinsame Varianzanteile mit allen drei Faktoren zeigt jedoch, im Gegensatz zu den anderen drei, keine signifikanten direkten Effekte auf das Verhalten. Es scheint so, dass die Varianzanteile in der Einstellung die normalerweise einen Zusammenhang mit dem Verhalten bewirken, durch die anderen drei Faktoren besser erklärt werden. Das bedeutet, dass die spezifischen Privatsphäre-Bedenken, die subjektiven Vorteile sowie die subjektive Sensitivität der Daten bereits alle Informationen zur Verhaltensvorhersage enthalten, die sonst von der Einstellung als

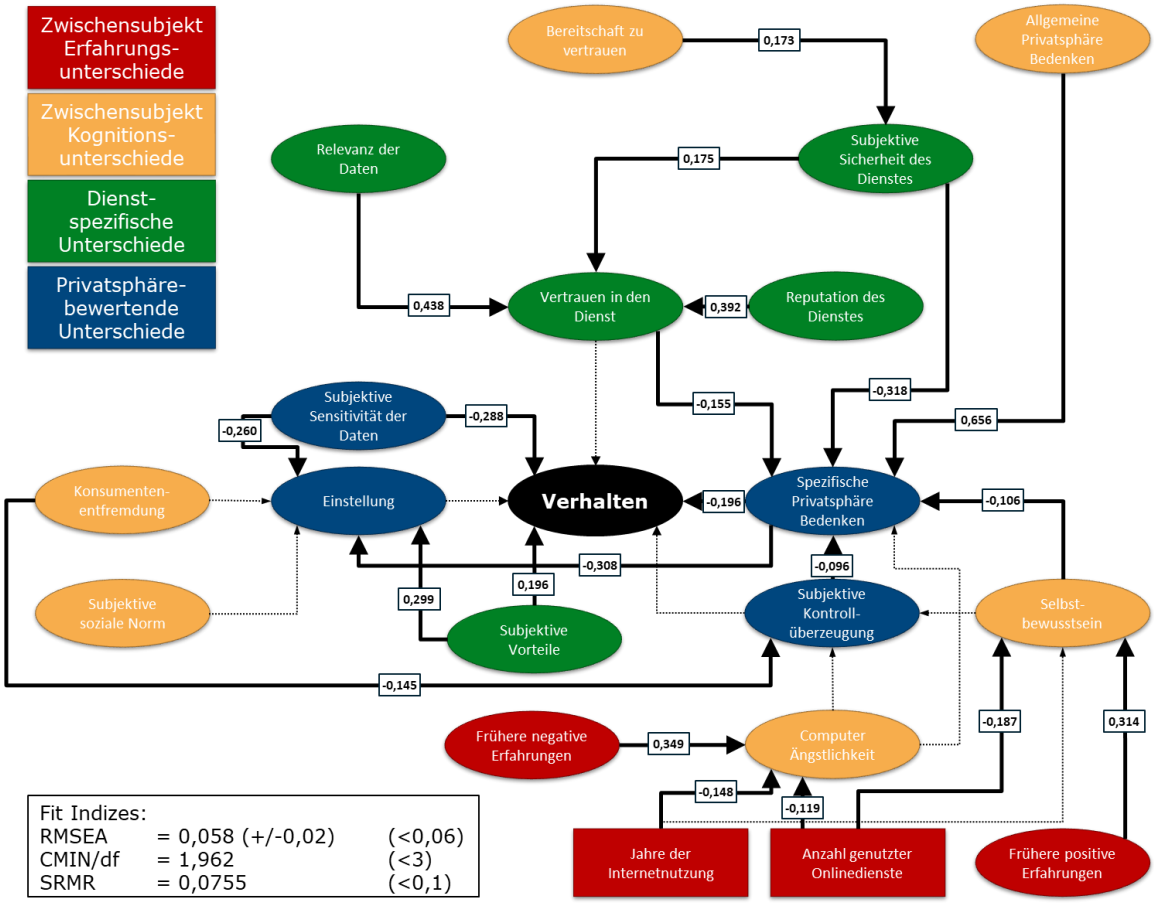

Abbildung 18. Hypothesenprüfung des Forschungsmodells; signifikante Hypothesen sind mit standardisierten Regressionsgewichten und durchgezogenen Pfeilen eingetragen; nicht bestätigte Hypothesen mit gestrichelten Pfeilen

Konstrukt beigesteuert werden. Diese drei Faktoren erklären die gleichen Varianzanteile besser, als es die Einstellung alleine kann.

Tabelle 8. Übersicht über die geprüften Hypothesen inklusive der standardisierten Regressionsgewichte und der zugehörigen p-Werte; fette Schreibweise der Wirkrichtung impliziert eine unterstützte Hypothese, normale Schreibweise einen nicht signifikanten Zusammenhang, kursiv einen signifikanten Zusammenhang entgegen der postulierten Wirkrichtung

	Postulierte Wirkrichtung	Standardisiertes β-Gewicht	p-Wert
H_1	Jahre der Internetnutzung → Selbstbewusstsein	-0,006	0,92
H_2	*Anzahl genutzter Onlinedienste → Selbstbewusstsein*	-0,187	<0,01**
H_3	**Jahre der Internetnutzung → Computerängstlichkeit**	-0,148	0,02*
H_4	**Anzahl genutzter Onlinedienste → Computerängstlichkeit**	-0,119	0,05*
H_5	**Frühere positive Erfahrungen → Selbstbewusstsein**	0,314	<0,01**
H_6	**Frühere negative Erfahrungen → Computerängstlichkeit**	0,349	<0,01**
H_7	Selbstbewusstsein → subjektive Kontrolle	0,044	0,49
H_8	**Selbstbewusstsein → spezifische Privatsphäre-Bedenken**	-0,106	0,03*
H_9	Computerängstlichkeit → subjektive Kontrolle	0,066	0,34
H_{10}	Computerängstlichkeit → spezifische Privatsphäre-Bedenken	0,032	0,57
H_{11}	Konsumentenentfremdung → Einstellung	-0,062	0,28
H_{12}	**Konsumentenentfremdung → subjektive Kontrolle**	-0,145	0,04*
H_{13}	Subjektive soziale Norm → Einstellung	0,056	0,29
H_{14}	**Subjektive Sensitivität → Einstellung**	-0,260	<0,01**
H_{15}	**Subjektive Sensitivität → Privatsphäre-relevantes Verhalten**	-0,288	<0,01**
H_{16}	**Vertrauen in den Dienst → spezifische Privatsphäre-Bedenken**	-0,155	<0,01**
H_{17}	Vertrauen in den Dienst → Privatsphäre-relevantes Verhalten	0,020	0,80
H_{18}	**Subjektive Relevanz der Daten → Vertrauen in den Dienst**	0,438	<0,01**
H_{19}	**Subjektive Sicherheit des Dienstes → Vertrauen in den Dienst**	0,175	<0,01**
H_{20}	**Subjektive Sicherheit des Dienstes → spezifische Privatsphäre-Bedenken**	-0,318	<0,01**
H_{21}	**Bereitschaft zu vertrauen → subjektive Sicherheit des Dienstes**	0,173	0,02*
H_{22}	**Reputation des Dienstes → Vertrauen in den Dienst**	0,392	<0,01**
H_{23}	**Allgemeine Privatsphäre-Bedenken → Spezifische Privatsphäre Bedenken**	0,656	<0,01**
H_{24}	**Subjektive Kontrolle → Spezifische Privatsphäre Bedenken**	-0,096	0,04*
H_{25}	Subjektive Kontrolle → Privatsphäre-relevantes Verhalten	-0,027	0,67
H_{26}	**Spezifische Privatsphäre Bedenken → Einstellung**	-0,308	<0,01**
H_{27}	**Spezifische Privatsphäre Bedenken → Privatsphäre-relevantes Verhalten**	-0,196	0,01**
H_{28}	**Subjektive Vorteile → Privatsphäre-relevantes Verhalten**	0,196	0,02*
H_{29}	**Subjektive Vorteile → Einstellung**	0,299	<0,01**
H_{30}	Einstellung → Verhalten	-0,010	0,90

* signifikant auf dem 5% Niveau
** signifikant auf dem 1% Niveau

Somit kann erklärt werden, dass die in anderen allgemeineren Modellen (z.B. die Theorie des geplanten Verhaltens [36]) zu findenden Effekte der Einstellung auf das Verhalten in diesem spezifischeren Modell nicht gefunden werden. Das integrative Verhaltensmodell trägt an dieser Stelle zum besseren Verständnis der Struktur der Effekte bei, indem es diesen Effekt spezifischer mittels drei distinkter Faktoren erklärt. Darüber hinaus bietet es einen Erklärungsansatz für das Phänomen des Privatsphären Paradoxons, d.h. den fehlenden statistischen Zusammenhang zwischen Einstellung bzw. Intention und tatsächlichem Verhalten im Kontext von Privatsphäre-relevanten Verhalten. Werden die Faktoren auf spezifischerer und umfassenderer Ebene betrachtet, zeigen sich signifikante Zusammenhänge mit dem tatsächlichen Verhalten.

Ähnlich verhält es sich mit dem auf Basis der Theorie des geplanten Verhaltens [36] postulierten direkten Effektes der subjektiven Kontrolle auf das Verhalten, bzw. dem auf Basis des Risk-Trust-Modells [9], [66] vorhergesagten Zusammenhangs zwischen Vertrauen in den Dienst und dem Verhalten. Beide werden nicht signifikant, jedoch die direkten Effekte auf die spezifischen Privatsphäre-Bedenken sowie deren Zusammenhang mit dem Verhalten. Sowohl die subjektive Kontrollüberzeugung, also der subjektive Grad des Einflusses, den ein Individuum auf die Situation als Ganzes sowie den Ausgang bzw. die Konsequenzen nehmen kann, als auch das Vertrauen in den Dienst als solches wirken dabei mildernd auf mögliche Privatsphäre-Bedenken. Ähnlich zur auf allgemeinen Modellen wie der Theorie des geplanten Verhaltens basierenden Erwartung hinsichtlich des Effektes der Einstellung auf das Verhalten, zeigt sich auch bei der subjektiven Kontrollüberzeugung und dem Vertrauen in einen Dienst, dass ein komplexeres integratives Verhaltensmodell mehr Einblick in die Struktur der Effekte bietet.

Entgegen der Modellannahme hängt die subjektive Kontrollüberzeugung, zumindest in der erhobenen Stichprobe, jedoch nur von einem Teil der erhobenen Zwischensubjekt-Kognitionsunterschiede ab. Einzig die Konsumentenentfremdung weist, wie von Mady [57] angenommen, einen hemmenden Einfluss auf die subjektive Kontrollüberzeugung auf. Je entfernter und entfremdet sich ein Individuum fühlt, desto weniger Einfluss auf die Situation erwartet es auch, was letztlich den möglichen positiven Effekt der eigenen Kontrollüberzeugung auf die Privatsphäre-Bedenken negiert. Das allgemeine Selbstbewusstsein, d.h. wie positiv oder negativ ein Individuum die eigene Person sieht und bewertet, hängt nicht direkt mit der subjektiven Kontrollüberzeugung zusammen, es wirkt jedoch direkt signifikant mildernd auf die spezifischen Privatsphäre-Bedenken.

Auffällig ist, dass die Computerängstlichkeit in der erhobenen Stichprobe zwar starke Zusammenhänge mit früheren negativen Erfahrungen, sowie der Erfahrung im Onlinekontext, dargestellt durch die Jahre der Internetnutzung und die genutzten Onlinedienste, zeigt, jedoch entgegen den Funden von Schwaig et al. [53] weder mit der subjektiven Kontrollüberzeugung noch mit den spezifischen Privatsphäre-Bedenken signifikante Zusammenhänge aufweist. Eine mögliche Erklärung hierfür liegt in der Zusammensetzung der hier erhobenen Stichprobe. Es handelt sich durchweg um sehr erfahrene Anwender mit gering bis sehr gering ausgeprägter Computerängstlichkeit, wohingegen Schwaig et al. ihre Hypothese darauf stützten, dass Individuen mit mittel bis hochausgeprägter Computerängstlichkeit eher negativ auf Datensammlung reagieren. Durch das Fehlen von mittel bis hoch ängstlichen Teilnehmern, lassen sich entsprechende Zusammenhänge nicht auf Basis der hier berichteten Ergebnisse ausschließen.

Das Selbstbewusstsein wird primär durch frühere positive Erfahrungen geprägt [48]. Auch der Zusammenhang mit der Anzahl der genutzten Onlinedienste wird signifikant, ist jedoch

entgegengesetzt gerichtet. Je mehr Dienste genutzt werden, desto geringer ist das Selbstbewusstsein in der Stichprobe ausgeprägt. Denkbare Erklärungen könnten hier sein, dass sich im digitalen Kontext selbstbewusste Individuen durchaus der Gefahren vieler Dienste bewusst sind und sich im Zuge dessen auf weniger verschiedene Dienste beschränken und weniger erfahrene und weniger selbstbewusste mehr verschiedene Dienste ausprobieren, insbesondere wenn diese von Freunden oder Familienmitgliedern empfohlen werden. Auf Basis der vorliegenden Daten lässt sich jedoch keine detailliertere Einsicht in diese Wirkzusammenhänge erreichen, sodass weiterführende Forschung nötig erscheint.

Im Vergleich zu den bereits diskutierten Einflüssen auf die spezifischen Privatsphäre-Bedenken, Vertrauen in den Dienst, Selbstbewusstsein sowie subjektive Kontrolle, sind die Effekte der beiden weiteren im Modell gefundenen signifikanten Faktoren noch deutlich stärker. Die allgemeinen Privatsphäre-Bedenken haben hierbei den mit Abstand stärksten Effekt. Individuen mit im allgemeinen größeren Bedenken haben auch in der untersuchten Situation erhöhte Bedenken. Dennoch zeigt sich erneut (vgl. z.B. [65], [80], [81], [102]), dass beide Konstrukte nicht identisch sind und es zum Verständnis der Handlungen im Kontext digitaler Privatsphäre unabdingbar ist, sowohl allgemeine, als auch situationsspezifische Bedenken zu adressieren.

Der zweite Faktor, der maßgeblich auf die spezifischen Privatsphäre-Bedenken Einfluss nimmt, ist die subjektive Sicherheit des Dienstes. Erwartungsgemäß [73] sind die Bedenken kleiner, wenn der Dienst als sicherer wahrgenommen wird. Die subjektive Sicherheit adressiert hierbei primär zwei Komponenten der Privatsphäre-Bedenken, den unautorisierten Zugriff sowie die fehlerhafte, weil manipulierte, Speicherung bzw. Verarbeitung der Daten [53], [65]. Neben objektiv beurteilbaren Kriterien, z.B. einer mittels HTTPS-Protokoll verschlüsselten Kommunikation mit dem Server bei der Dateneingabe als Schutz gegen Manipulation und Zugriff durch Dritte während der Übertragung, spielt hierbei auch die grundsätzliche Bereitschaft eines Individuums zu vertrauen eine signifikante Rolle.

Die subjektive Sicherheit wirkt zusätzlich auch signifikant positiv auf das Vertrauen, das in den Dienst gesetzt wird. Insbesondere im digitalen Privatsphäre-relevanten Kontext wird hierbei die Fähigkeit-Komponente [61] des Vertrauens adressiert, d.h. hält das Individuum den Dienstanbieter für fähig, die erhobenen Daten korrekt und hinreichend abzusichern. Eine andere Komponente, die Integrität, d.h. die Überzeugung, dass der Dienstanbieter auf Basis von akzeptablen Prinzipien handelt [61], adressiert die Reputation des Dienstes. Genießt der Anbieter bekanntermaßen einen guten Ruf, so steigt das Vertrauen in ihn, da seine Handlungen allgemein akzeptiert und erwünscht erscheinen. Die Relevanz der Daten schließlich adressiert sowohl die Integrität als auch die dritte Komponente, das Wohlwollen. Sind die durch den Anbieter erfragten Daten sinnhaft mit den gebotenen Diensten oder Funktionalitäten verknüpft und werden nicht unnötige persönliche Daten erhoben, so wirkt der Anbieter integer und scheint nicht, oder nicht primär, egozentrischen profitorientierten Motiven zu folgen, was sich ebenfalls positiv auf das Vertrauen auswirkt, welches dem Dienst entgegengebracht wird.

4.4.1. Implikationen für die Forschung

Das hier vorgestellte integrative Verhaltensmodell zeigt, dass der stärkste Prädiktor für Privatsphäre-relevantes Verhalten die subjektive Sensitivität der Daten ist. Erscheinen diese auf den ersten Blick für eine mögliche Intervention zur Verbesserung des Privatsphäre-relevanten Verhaltens

(d.h. zum besseren Selbstschutz der individuellen Privatsphäre) weniger relevant, da sie schwerlich zu modifizieren sind, so bergen sie auf den zweiten Blick jedoch durchaus Potential.

In den letzten zehn Jahren zeigten viele publizierte Studienergebnisse aus der Privatsphäre-Forschung, dass Anwender vor allem ein Mangel an Verständnis und Bewusstsein gegenüber technischen Vorgängen und Zusammenhängen zeigen (z.B. [14], [18], [19], [25], [103]). Dabei werden sowohl Usability-Probleme als auch fehlendes Wissen oder Aufmerksamkeit als mögliche Ursachen diskutiert und identifiziert. Die hier berichteten Ergebnisse unterstreichen dies. Anwender berücksichtigen in ihren Entscheidungen durchaus in starkem Maße, ob erhobene Daten eine Verletzung der eigenen Privatsphäre darstellen. Um dies jedoch stets zu tun müssen sie dafür wissen, welche Daten überhaupt erhoben werden und, insbesondere bei eher technischen Daten wie z.B. IP-Adressen, was diese bedeuten. Ähnliche Überlegungen treffen auch auf die Bewertung der Relevanz der Informationen zu. Ist dies unter Umständen im Kontext einer Umfrage, wie in dieser Studie, noch für eine breite Masse zu beantworten, ist es beispielsweise im Kontext der Auswahl von Smartphone Applikationen stark davon abhängig, wie diese Informationen aufbereitet und dargestellt werden [22].

Es gilt weiterhin intensiv zu untersuchen, wie der Anwender möglichst immer gut darüber informiert werden kann, welche Daten zu welchem Zeitpunkt zu wem fließen, sodass dieser für ihn möglichst gute, d.h. zu seinen Wünschen passende, Entscheidungen treffen kann.

4.4.2. Implikationen für die Praxis

Im Kontext des integrativen Verhaltensmodells bieten sich für Dienstanbieter vor allem die dienstspezifischen Faktoren als Ansatzpunkte an. Insbesondere die Förderungen des Vertrauens in den Dienst ist eine augenscheinlich offensichtliche Methode, um Nutzern ihre möglicherweise ungerechtfertigten Privatsphäre-Bedenken zu nehmen. Aus praktischer Sicht, abseits von klassischen PR-Kampagnen zur Verbesserung der Reputation, bieten sich hierbei vor allem die Relevanz der Daten sowie die subjektive Sicherheit an.

In Bezug auf die Relevanz der Daten gilt es zum einen sich auf die Daten zu beschränken, die auch wirklich benötigt werden. Genügt die Einordnung in einer Altersgruppe, so sollte auch entsprechend nur diese erhoben werden und nicht das exakte Alter. Genügt ein Session-Cookie so muss beim Anwender keiner mit einer Lebenszeit von mehreren Jahren platziert werden. Zum anderen gilt es aber auch, die subjektive Komponente auf der Seite des Anwenders im Blick zu behalten. Der Anwender muss wissen, dass die erhobenen Daten für die Diensterbringung relevant sind. Es gilt also hier in knappen und klaren Worten dem Anwender verständlich zu machen, welche Daten zu welchem Zweck erhoben werden und warum diese notwendig sind. Auch ein einfach zugänglicher Überblick über die bereits erhobenen und gespeicherten Daten kann, je nach Dienstkontext, hier hilfreich sein, um den Anwender mehr Kontrolle zu vermitteln und einen subjektiv fairen Informationsfluss zu ermöglichen [104].

Für die subjektive Sicherheit gilt es vor allem, klar und vollständig zu kommunizieren, wie die erhobenen Informationen gegen Zugriff und Missbrauch durch Dritte geschützt werden, welche Konsequenzen zu erwarten sind, wenn diese Informationen (nicht) weitergegeben werden und welche Rechtshilfen und Entschädigungen ggf. zu erwarten sind [8], [70]. Hierbei empfiehlt es sich v.a. auch nicht nur auf die Datenschutzrichtlinien zu vertrauen, die im Allgemeinen so juristisch und ausführlich geschrieben sind, dass Anwender diese bestenfalls überfliegen, zumeist jedoch vorher schon aufgeben. Eine stichwortartige Zusammenfassung der wesentlichen Punkte bereits vor der Anzeige

von Datenschutzrichtlinie oder Allgemeinen Geschäftsbedingungen kann hier vertrauensfördernd wirken, da diese essentiellen Informationen so erst in einer Entscheidung berücksichtig werden können. Dies gilt insbesondere, wenn hier Eigenschaften vorliegen, die den eigenen Dienst von Konkurrenzunternehmen abheben und somit als Alleinstellungsmerkmal verkaufsfördernd beziehungsweise umsatzstärkend wirken können.

4.4.3. Limitationen

Obwohl sich das integrative Verhaltensmodell in der Studie als robust und passend erwiesen hat, gilt es einige Limitationen zu beachten. Hierzu gehört zunächst vor allem das gewählte Szenario der freiwilligen Datenabfrage im Kontext einer wissenschaftlichen Studie. Die Wahrnehmung der Anwender von Unternehmen oder staatlichen Institutionen könnte sich von der Wahrnehmung einer Umfrageseite oder einer Universität deutlich unterscheiden. Darüber hinaus könnten sich Unterschiede hinsichtlich des Entscheidungsverhaltens beziehungsweise der entscheidungsbildenden Faktoren zeigen, wenn keine explizite Informationsweitergabe, wie in dieser Studie oder beispielsweise bei der Account-Registrierung und der Facebook-Nutzung betrachtet wird, sondern Informationen oder Daten implizit weitergegeben werden und damit schwerer für den Anwender erkennbar sind. Ein Beispiel hierfür könnte das Tracking des Surf-Verhaltens mittels Cookies sein.

Darüber hinaus gilt es zu beachten, dass es auf Grund der Gestaltung der Studie nicht möglich ist, die Angabe von falschen Informationen zu identifizieren. Zum Schutz der Privatsphäre der Teilnehmer wurden die bereitgestellten Informationen nicht gesichtet und eventuell auf Korrektheit geprüft, sondern direkt maskiert und anonymisiert. Teilnehmer könnten also unter Umständen zum Beispiel falsche Informationen über ihr Gehalt, ihre Herkunft oder auch ihre Gesundheit gemacht haben, ohne dass dies im Kontext dieser Studie nachprüfbar wäre. Eine solche Prüfung würde jedoch, soweit überhaupt möglich, eine vollständige De-Anonymisierung der Teilnehmer erfordern, was aus ethischen Gesichtspunkten im Rahmen dieser Arbeit nicht angemessen erschien.

Des Weiteren zeichnet sich die Stichprobe zum einen dadurch aus, dass ausschließlich Einwohner der Vereinigten Staaten von Amerika erhoben wurden und zum anderen, dass sie durchweg sehr erfahren im Onlinekontext waren und, damit einhergehend, nur geringe bis sehr geringe Werte in Bezug auf Computerängstlichkeit aufwiesen. Eine weitere Studie mit einer in diesen Eigenschaften heterogeneren Stichprobe bzw. eine Replikation derselben Studie mit zusätzlichen Probanden mit entsprechenden Eigenschaften, könnte zu weiteren und vor allem allgemeingültigeren Ergebnissen führen.

5. Rückblick und Ausblick

Die Ziele der vorliegenden Arbeit waren zunächst, die Probleme und Schutzmöglichkeiten des digitalen Alltags für Endanwender zu betrachten, einen Interface-Prototypen zu Verbesserung der Informationslage von Endanwendern im digitalen Alltag zu entwickeln und zu evaluieren sowie auf Basis der daraus gewonnenen Erkenntnisse und einer umfangreichen Literaturrecherche ein integratives Verhaltensmodell zu formulieren und zu überprüfen.

Bei der Betrachtung von Problemen und Schutzmöglichkeiten im digitalen Alltag und bei der Nutzung von Smartphones im Speziellen, zeigten sich insbesondere die Berechtigungsdarstellungen der mobilen Betriebssysteme als vielversprechender und notwendiger Ansatzpunkt. Experten äußerten im Interview (vgl. Kapitel 2.1) die Empfehlung, dass Anwender bei der Wahl von Applikationen für ihr Smartphone insbesondere die angeforderten Berechtigungen darauf prüfen sollten, ob sie im Kontext der gebotenen Funktionalität sinnhaft und im Kontext der eigenen Bedürfnisse akzeptabel sind.

Gleichzeitig zeigte eine Betrachtung der aktuellen Berechtigungsdarstellungen sowie von Forschungsergebnissen diesbezüglich (vgl. Kapitel 2.2 und 2.3), dass der typische Anwender hier mehr Unterstützung benötigt. In der Praxis von Android wurde hierbei insbesondere die Abstraktion, d.h. die Reduktion, der dargestellten Informationen mit dem Ziel der Verbesserung der Verständlichkeit der Darstellung als Lösungsweg eingeschlagen. Diesen nutzten auch einige Forscher in ihren Alternativvorschlägen [26], [27].

Die im Kontext dieser Arbeit entwickelte Berechtigungsdarstellung „COPING“ verfolgte dem entgegengesetzt einen Weg mit dem Ziel, die dargestellten Informationen nicht zu reduzieren, sondern mit zusätzlichen Informationen anzureichern und so zu strukturieren, dass die Informationen nützlicher werden. Auf diese Weise konnte eine Verbesserung der Entscheidungsqualität in Hinblick auf die Privatsphäre bei den Teilnehmern der Evaluationsstudie beobachtet werden. Diese zeigte sich insbesondere bei der Betrachtung einer komplexen und bewusst täuschend konstruierten Entscheidungssituation, die ein Verständnis des angeforderten Berechtigungssets erforderte und nicht mit einfachen Abzähl-Heuristiken („weniger ist besser“) gelöst werden konnte.

Da „COPING“ in der Studie die komplexeste Darstellung war, kann nicht abschließend beantwortet werden, ob damit bereits eine Sättigung auf Seiten des Anwenders erreicht ist, oder ob eine weitere Anreicherung mit nützlichen Informationen die Darstellung und, damit einhergehend, die Entscheidungsgüte weiter verbessern würde. Denkbare Ergänzungen hierbei sind zum Beispiel weiterführende Informationen zu Datenflüssen, sodass nicht nur bewertbar ist, auf welche Daten eine Applikation potentiell zugreifen könnte, sondern auch, worauf sie tatsächlich zugreift und wer diese Daten empfängt. Erste Prototypen für solche Ergänzungen wurden zum Beispiel im Kontext des Projektes ZertApps[39] untersucht.

Hierbei gilt es, einen Kompromiss zwischen Verständlichkeit der Darstellung sowie der Komplexität bzw. dem Umfang der dargestellten Informationen zu finden. Während sich eine simple Abstraktion, d.h. die Reduktion der gebotenen Informationen, als unzureichend und nicht zielführend erwies, bleibt es unklar, wieviel mehr an Informationen geboten werden kann, ohne dass die Entscheidungsqualität

[39] http://www.zertapps.de/

durch zu hohe Komplexität oder zu großen Verarbeitungsaufwand auf Seiten des Anwenders erneut geschmälert wird.

Das im weiteren Verlauf der Arbeit (vgl. Kapitel 4) formulierte integrative Verhaltensmodell zeigt auf Basis von Forschungsliteratur und den vorherigen Erkenntnissen eine Struktur, d.h. Wirkzusammenhänge, von insgesamt 19 verschiedenen Faktoren für die Verhaltensbildung bzw. Entscheidungsfindung bei Privatsphäre-relevantem Verhalten auf. Es zeigt sich robust, weist gute Fit-Werte auf und bietet somit einen Erklärungsansatz für die oben beschriebene Beobachtung.

Bessere Informationen, wie sie z.B. „COPING" im Kontext der Bewertung von Berechtigungen bei der Applikationswahl bietet, führen zu besseren Entscheidungen. Hierbei adressiert „COPING" vor allem die beiden Faktoren der subjektiven Sensitivität sowie der Relevanz der Daten. Die Darstellung zeigt im Einzelnen auf, welche Berechtigungen durch die Applikation angefordert werden und ob diese im Kontext der gebotenen Funktionalität sinnvoll und notwendig sind. Erst die Kenntnis dieser Informationen ermöglicht es, die Sensitivität der Daten in der individuellen Entscheidung zu berücksichtigen, da hierfür bekannt sein muss, auf welche Daten im Einzelnen zugegriffen werden könnte.

Über den Anwendungsfall im Kontext von „COPING" hinaus illustriert das Verhaltensmodell auch sehr eindrucksvoll das sogenannte Privatsphären Paradoxon, die Beobachtung, dass kein statistischer Zusammenhang zwischen der Einstellung und dem eigentlichen real gezeigten Verhalten beobachtbar ist. Dies erscheint hier jedoch nicht paradox, da über dieses allgemeine Konstrukt hinaus weitere Faktoren betrachtet wurden. Das reale Verhalten zeigt im Modell direkte unmittelbare signifikante Zusammenhänge mit den spezifischen Privatsphäre-Bedenken, den subjektiven Vorteilen und vor allem mit der subjektiven Sensitivität der Daten. Alle drei weisen ebenfalls signifikante Zusammenhänge mit der Einstellung auf, die Konstrukte enthalten also zum Teil ähnliche Informationen, einzelne Facetten der Einstellung sind jeweils auch in den subjektiven Vorteilen, den spezifischen Privatsphäre-Bedenken sowie der subjektiven Sensitivität enthalten. Werden diese Facetten getrennt betrachtet, statt sie in ein Konstrukt zu subsummieren, löst sich das Paradoxon und es zeigen sich signifikante Zusammenhänge mit dem real gezeigten Verhalten.

Darüber hinaus zeigen beispielsweise das Vertrauen in den Dienst, das Selbstbewusstsein, die subjektive Kontrolle oder die Konsumentenentfremdung mittelbare Effekte auf das Verhalten. Der Prozess der Verhaltensbildung ist ein komplexer, von vielen, auch situativen, Variablen beeinflusster Vorgang. Entsprechend müssen auch sowohl situative als auch zeitstabile Faktoren untersucht und erforscht werden, um diesen Prozess besser zu verstehen und menschliches Verhalten auch in so spezifischen Situationen wie zum Beispiel der Wahl von Smartphone Applikationen besser erklären zu können.

Literaturverzeichnis

[1] D. Nafus and K. Tracey, "Mobile phone consumption and concepts of personhood," in *Perpetual Contact: Mobile Communication, Private Talk, Public Performance*, J. Katz and M. Aakhus, Eds. Cambridge: University Press, 2002, p. 206.

[2] R. S. Ling, *New tech, new ties*. MIT press Cambridge, MA, 2008.

[3] I. Liccardi, J. Pato, and D. J. Weitzner, "Improving mobile app selection through transparency and better permission analysis," *Journal of Privacy and Confidentiality*, vol. 5, no. 2, pp. 1–55, 2013.

[4] C. J. Bennett, "The political economy of privacy: a review of the literature," *Hackensack, NJ: Center for Social and Legal Research*, 1995.

[5] A. Westin, "Privacy and freedom.," *Atheneum, New York*, 1967.

[6] F. D. Schoeman, *Philosophical dimensions of privacy: An anthology*. Cambridge University Press, 1984.

[7] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review," *MIS quarterly*, vol. 35, no. 4, pp. 989–1016, 2011.

[8] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, vol. 10, no. 1, pp. 104–115, 1999.

[9] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *The Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[10] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122–134, Jan. 2017.

[11] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE Security & Privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[12] D. Boyd and N. Ellison, "Social network sites: Definition, history, and scholarship," *IEEE Engineering Management Review*, vol. 3, no. 38, pp. 16–31, 2010.

[13] A. Deuker, "Addressing the privacy paradox by expanded privacy awareness – The example of context-aware services," in *Privacy and Identity Management for Life*, M. Bezzi, P. Duquenoy, S. Fischer-Hübner, G. Zhang, and M. Hansen, Eds. Springer, 2010, pp. 275–283.

[14] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, "A socio-technical investigation into smartphone security," in *International Workshop on Security and Trust Management*, 2015, pp. 265–273.

[15] S. Pötzsch, "Privacy awareness: A means to solve the privacy paradox?," in *The Future of Identity in the Information Society*, vol. 298, V. Matyáš, S. Fischer-Hübner, D. Cvrcek, and P. Švenda, Eds. Berlin, Heidelberg: Springer, 2009, pp. 226–236.

[16] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson, "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, 2014, pp. 2347–2356.

[17] O. Kulyk, P. Gerber, M. El Hanafi, B. Reinheimer, K. Renaud, and M. Volkamer, "Encouraging privacy-aware smartphone app installation: What would the technically-adept do?," in *Usable Security Workshop*, 2016.

[18] A. P. Felt, S. Egelman, and D. Wagner, "I've Got 99 Problems, but vibration ain't one: A survey of smartphone users' concerns," in *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2012, pp. 33–44.

[19] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: Installing applications on an android smartphone," in *Proceedings of the 16th international Conference on Financial Cryptography and Data Security*, 2012, pp. 68–79.

[20] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the 8th Symposium on Usable Privacy and Security*, 2012, p. 3:1—–3:14.

[21] P. Gerber, M. Volkamer, and K. Renaud, "Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy," *ACM SIGCAS Computers and Society*, vol. 45, no. 1, pp. 16–21, 2015.

[22] P. Gerber, M. Volkamer, and K. Renaud, "The simpler, the better? Presenting the COPING Android permission-granting interface for better privacy-related decisions," *Journal of Information Security and Applications*, vol. 34, pp. 8–26, 2017.

[23] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2011, pp. 3–14.

[24] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009, pp. 235–245.

[25] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 2011, pp. 627–638.

[26] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2013, pp. 3393–3402.

[27] L. Kraus, I. Wechsung, and S. Möller, "Using statistical information to communicate android permission risks to users," in *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on*, 2014, pp. 48–55.

[28] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 2012, pp. 501–510.

[29] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *Proceedings of the 32nd annual ACM Conference on Human Factors in Computing Systems*, 2014, pp. 2647–2656.

[30] N. Wang, B. Zhang, B. Liu, and H. Jin, "Investigating effects of control and ads awareness on Android users' privacy behaviors and perceptions," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, 2015, pp. 373–382.

[31] A. P. Felt, S. Egelman, M. Finifter, D. Akhawe, and D. Wagner, "How to ask for permission," in *Presented as Part of the 7th USENIX Workshop on hot Topics in Security*, 2012.

[32] G. Gigerenzer and U. Hoffrage, "How to improve Bayesian reasoning without instruction: Frequency formats," *Psychological Review*, vol. 102, no. 4, p. 684, 1995.

[33] ISO, "Standard Graphical Symbols: Safety Colours and Safety Signs–Registered Safety Signs (ISO 7010: 2003). 2003," *International Standards Organisation (ISO): Geneva, Switzerland*.

[34] N. Good, R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, and J. Konstan, "Stopping spyware at the gate: A user study of privacy, notice and spyware," in *Proceedings of the 2005 Symposium on Usable Privacy and Security*, 2005, pp. 43–52.

[35] N. Gerber, P. Gerber, and M. Volkamer (submitted), "Explaining the Privacy Paradox - A systematic review of literature investigating privacy attitude and behavior," *Computers & Security*.

[36] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processess*, vol. 50, no. 2, pp. 179–211, 1991.

[37] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," *Psychological Review*, vol. 84, no. 2, p. 191, 1977.

[38] A. Bandura, "Social cognitive theory of self-regulation," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 248–287, 1991.

[39] A. Bandura, "Self-efficacy mechanism in human agency.," *American Psychologist*, vol. 37, no. 2, p. 122, 1982.

[40] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[41] D. L. Floyd, S. P. Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory," *Journal of Applied Social Psychology*, vol. 30, no. 2, pp. 407–429, 2000.

[42] C. Flender and G. Müller, "Type indeterminacy in privacy decisions: The privacy paradox revisited," *Springer-Verlag Berlin Heidelberg*, vol. 7620 LNCS, pp. 148–159, 2012.

[43] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, vol. 17, no. 1, pp. 61–80, 2006.

[44] R. T. Rust, P. K. Kannan, and N. Peng, "The customer economics of Internet privacy," *Journal of the Academy of Marketing Science*, vol. 30, no. 4, pp. 455–464, 2002.

[45] N. Farag Awad and M. S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly*, vol. 30, no. 1, pp. 13–28, 2006.

[46] P. Greenfield and Z. Yan, "Children, adolescents, and the Internet: A new field of inquiry in developmental psychology.," *Developmental Psychology*, vol. 42, no. 3, p. 391, 2006.

[47] C. Steinfield, N. B. Ellison, and C. Lampe, "Social capital, self-esteem, and use of online social network sites: A longitudinal analysis," *Journal of Applied Developmental Psychology*, vol. 29, no. 6, pp. 434–445, 2008.

[48] E. L. Deci and R. M. Ryan, "Human agency: The basis for true self-esteem. In MH Kemis (Ed.), Efficacy, agency, and self-esteem (pp. 31-50)." New York: Plenum, 1995.

[49] E. Greenberger, C. Chen, J. Dmitrieva, and S. P. Farruggia, "Item-wording and the dimensionality of the Rosenberg Self-Esteem Scale: Do they matter?," *Personality and Individual Differences*, vol. 35, no. 6, pp. 1241–1254, Oct. 2003.

[50] T. A. Judge and T. N. Bauer, "Personality and work role affect," in *Paper presented at the annual Meeting of the Academy of Management*, 1997.

[51] K. M. Ruggiero and D. M. Taylor, "Why minority group members perceive or do not perceive the discrimination that confronts them: The role of self-esteem and perceived control.," *Journal of Personality and Social Psychology*, vol. 72, no. 2, p. 373, 1997.

[52] C. Liu, J. T. Marchewka, J. Lu, and C.-S. Yu, "Beyond concern - A privacy-trust-behavioral intention model of electronic commerce," *Information & Management*, vol. 42, no. 2, pp. 289–304, 2005.

[53] K. S. Schwaig, A. H. Segars, V. Grover, and K. D. Fiedler, "A model of consumers' perceptions of the invasion of information privacy," *Information & Management*, vol. 50, no. 1, pp. 1–12, 2013.

[54] A. C. Raub, "Correlates of computer anxiety in college students," University of Pennsylvania, 1981.

[55] E. B. Johnson, "Cognitive age: Understanding consumer alienation in the mature market," *Review of Business*, vol. 17, no. 3, p. 35, 1996.

[56] F. K. Shuptrine, "On the validity of using students as subjects in consumer behavior investigations," *The Journal of Business*, vol. 48, no. 3, pp. 383–390, 1975.

[57] T. T. Mady, "Sentiment toward marketing: Should we care about consumer alienation and readiness to use technology?," *Journal of Consumer Behaviour*, vol. 10, no. 4, pp. 192–204, 2011.

[58] H. O. Pruden, F. K. Shuptrine, and D. S. Longman, "A measure of alienation from the marketplace," *Journal of the Academy of Marketing Science*, vol. 2, no. 1–4, pp. 610–619, 1974.

[59] A. Beldad, M. De Jong, and M. Steehouder, "I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions," *Computers in Human Behavior*, vol. 27, no. 6, pp. 2233–2242, 2011.

[60] J. Song and F. M. Zahedi, "Trust in health infomediaries," *Decision Support Systems*, vol. 43, no. 2, pp. 390–407, Mar. 2007.

[61] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.

[62] C. M. K. Cheung and M. K. O. Lee, "Understanding consumer trust in Internet shopping: A multidisciplinary approach," *Journal of the American Society for Information Science and Technology*, vol. 57, no. 4, pp. 479–492, Feb. 2006.

[63] J. K. Butler Jr, "Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory," *Journal of Management*, vol. 17, no. 3, pp. 643–663, 1991.

[64] K. Giffin, "The contribution of studies of source credibility to a theory of interpersonal trust in the communication process," *Psychological Bulletin*, vol. 68, no. 2, p. 104, 1967.

[65] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research*, vol. 15, no. 4, pp. 336–355, 2004.

[66] G. R. Milne and M.-E. Boza, "Trust and concern in consumers' perceptions of marketing information management practices," *Journal of interactive Marketing*, vol. 13, no. 1, pp. 5–24, 1999.

[67] T. Donaldson and T. W. Dunfee, "Toward a unified conception of business social ethics: Integrative contracts theory," *The Academy of Management Review*, vol. 19, no. 2, pp. 252–284, 1994.

[68] G. R. Milne and M. E. Gordon, "Direct mail privacy-efficiency trade-offs within an implied social contract framework," *Journal of Public Policy & Marketing*, vol. 12, no. 2, pp. 206–215, 1993.

[69] E. F. Stone and D. L. Stone, "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms," *Research in Personnel and Human Resources Management*, vol. 8, no. 3, pp. 349–411, 1990.

[70] G. Bansal, F. M. Zahedi, and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, vol. 49, no. 2, pp. 138–150, 2010.

[71] M. J. Culnan and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, vol. 10, no. 1, pp. 104–115, 1999.

[72] M. Igbaria, "User acceptance of microcomputer technology: An empirical test," *Omega*, vol. 21, no. 1, pp. 73–90, 1993.

[73] M. S. Featherman and P. A. Pavlou, "Predicting e-services adoption: A perceived risk facets perspective," *International Journal of Human-Computer Studies*, vol. 59, no. 4, pp. 451–474, 2003.

[74] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "Social influence, social interaction, and social psychology in the study of trust," *Academy of Management Review*, vol. 21, no. 2, p. 337, 1996.

[75] D. L. Paul and R. R. McDaniel Jr, "A field study of the effect of interpersonal trust on virtual collaborative relationship performance," *MIS Quarterly*, pp. 183–227, 2004.

[76] P. M. Doney and J. P. Cannon, "An examination of the nature of trust in buyer-seller relationships," *Journal of Marketing*, vol. 61, no. 1, pp. 35–51, 1997.

[77] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research*, vol. 13, no. 3, pp. 334–359, 2002.

[78] S. L. Jarvenpaa, N. Tractinsky, and L. Saarinen, "Consumer trust in an internet store: A cross-cultural validation," *Journal of Computer-Mediated Communication*, vol. 5, no. 2, pp. 1–34, 1999.

[79] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393–404, 1998.

[80] H. Li, R. Sarathy, and H. Xu, "Understanding situational online information disclosure as a privacy calculus," *Journal of Computer Information Systems*, vol. 51, no. 1, pp. 62–71, 2010.

[81] Y. Li, "The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns," *Decision Support Systems*, vol. 57, no. 1, pp. 343–354, 2014.

[82] I. Ajzen and M. Fishbein, "The influence of attitudes on behavior," in *The Handbook of Attitudes*, D. Albarracín, B. T. Johnson, and M. P. Zanna, Eds. Mahwah, NJ: Lawrence Erlbaum Associates, 2005, pp. 173–221.

[83] A. Bandura, "Social cognitive theory : An agentic perspective," *Annual Review of Psychology*, vol. 52, no. 1, pp. 1–26, 2001.

[84] H. Liang and Y. Xue, "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly*, vol. 33, no. 1, pp. 71–90, 2009.

[85] H. Xu, H. Teo, B. C. Y. Tan, and R. Agarwal, "Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns : A study of location-based services," *Information Systems Research*, vol. 23, no. 4, pp. 1342–1363, 2012.

[86] M. Fishbein and I. Ajzen, *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis, 2011.

[87] Y. Li, "A multi-level model of individual information privacy beliefs," *Electronic Commerce Research and Applications*, vol. 13, no. 1, pp. 32–44, 2014.

[88] G. Kirchgässner, *Homo oeconomicus: Das ökonomische Modell individuellen Verhaltens und seine Anwendung in den Wirtschafts- und Sozialwissenschaften*. Tübingen: Mohr, 1991, p. 362.

[89] V. H. Vroom, *Work and Motivation*. New York: John Willey & Sons, 1964.

[90] A. Kittur, E. H. Chi, and B. Suh, "Crowdsourcing user studies with Mechanical Turk," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2008, pp. 453–456.

[91] N. Gerber, "Was motiviert Nutzer? Nutzungsziele und Bedürfnisse," in *Zweiter Workshop des MoPPa Projektes*, 2017.

[92] D. Gefen, "E-commerce: The role of familiarity and trust," *Omega*, vol. 28, no. 6, pp. 725–737, 2000.

[93] D. H. Shin and Y. J. Shin, "Why do people play social network games?," *Computers in Human Behavior*, vol. 27, no. 2, pp. 852–861, 2011.

[94] H. Li, R. Sarathy, and H. Xu, "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors," *Decision Support Systems*, vol. 51, no. 3, pp. 434–445, Jun. 2011.

[95] H. Xu, T. Dinev, H. J. Smith, and P. Hart, "Examining the formation of individual's privacy concerns: Toward an integrative view," in *Proceedings of the international Conference on Information Systems*, 2008, pp. 1–14.

[96] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[97] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, p. 39, Feb. 1981.

[98] P.-W. Lei and Q. Wu, "Introduction to structural equation modeling: Issues and practical considerations," *Educational Measurement: Issues and Practice*, vol. 26, no. 3, pp. 33–43, Sep. 2007.

[99] L. Hu and P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A multidisciplinary Journal*, vol. 6, no. 1, pp. 1–55, 1999.

[100] J. H. Steiger, "Statistically based tests for the number of common factors," *Paper presented at the annual Meeting of the Psychometric Society, Iowa City, IA*, 1980.

[101] P. M. Bentler, *EQS structural equations program manual*. Multivariate Software, 1995.

[102] Y. Li, "Empirical studies on online information privacy concerns: Literature review and an integrative framework," *Communications of the Association for Information Systems*, vol. 28, no. 1, pp. 453–496, 2011.

[103] F. Shirazi and M. Volkamer, "What deters Jane from preventing identification and tracking on the web?," *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pp. 107–116, 2014.

[104] E. A. Lind and T. R. Tyler, *The social psychology of procedural justice*. New York, NY 10013: Plenum Press, 1988, p. 267.

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang

A1. Interviewstudie zur Ableitung von Heuristiken

[Zugehöriger Inhalt in Kapitel 2.1 ab Seite 13]

Qualifikation

- Wissen über
  - Mobile OS
  - Mobile Security
  - App Security
  - Professional Research ODER
  - Persönliches Interesse / Nutzer Erfahrung
- Wie lange schon ……. Jahre
- Welche Detailtiefe? [Offen]

Persönliche Erfahrung

- Welches Betriebssystem verwendest du i.A.? - tendenziell kürzer fassen
  - Wie lange? (Zeit und Geräte; ggf. warum **Wechsel**?)
  - Welche Version?
  - (ggf. rooted?)
- Hast du ein Gerät für **Arbeit und Privates**, oder jeweils getrennt?
  [Warum; Welche Form (Dual Sim o.ä.); falls zwei, welches wird häufiger genutzt?]
- Was machst du mit deinem **Hauptgerät üblicherweise** so?
  [ggf. interessante Tasks näher ausführen]
  - Wie viele Apps hast du in etwa selbst auf deinem Gerät installiert …… (Anzahl)
  - Wie oft suchst du / installierst du neue Apps? …… (Frequenz)
    [Hast du dabei bestimmte Kriterien zur Auswahl?; Vorgehen etc. … **Überleitung** zur Task]

App Installation

- Wir haben eine kleine Aufgabe für dich: Bitte suche (ca. 5 Minuten) nach einer neuen App zum Sudoku spielen / zur Bildbearbeitung
  - Bitte geh dabei so vor, wie du **üblicherweise** auch nach einer App suchen würdest
  - Versuche dabei deine Gedankengänge / Ideen / Assoziationen laut auszusprechen (**Think-Aloud**) während du dir verschiedene Apps aussuchst
  - Lege dein Telefon dabei nach Möglichkeit so, dass wir auch etwas sehen können
  - Du musst am Ende die App nicht unbedingt auf deinem Gerät installieren, nur soweit, bis du sagen würdest 'ja diese App würde ich jetzt mit dem letzten Tastendruck installieren' (oder falls keine gefunden begründen, warum keine dabei war)
  - Ca. **5 Minuten**
  - **Tasks:**
    - Sudoku („Prozess jetzt abgeschlossen?“ → Dann nächster Task)
    - Bildbearbeitung - Angenommen du suchst jetzt eine Bildbearbeitungs-App …
      - Mindestfunktionen:
        - Bilder / Fotos vom Gerät öffnen können
        - Verschiedene Filter anwenden können
        - Einfache Bearbeitung (Drehen, Zuschneiden, etc.)
        - Ergebnis speichern / Teilen per Mail o.ä.
- Besprechung des Vorgehens bei der App suche …
  - Welche **Kriterien** waren entscheidend (sowohl für, als auch gegen eine App!)?
  - Hast du bestimmte Hinweise / Bereiche des Interface besonders genutzt?

- **Permissions** / Freigaben (iOS) beachtet? Falls ja, welche waren wichtig? Welche nicht so? Falls nein, warum nicht?
- Anderen Store genutzt?
- Dritte Quellen (Google im Browser o.ä.) genutzt?
- Hast du hier (Bildbearbeitung) etwas anders gemacht, speziell beachtet, was ggf. bei anderen App Kategorien nicht der Fall ist?

Allgemeine Empfehlungen

- Was denkst du ist bei der Auswahl von Apps besonders wichtig? -
  - Empfehlungen für mich (Endanwender) … und für Oksana (Als Technikexpertin)
    - Wie schaut es mit InterApp-Datenflüssen aus? Ist es bekannt, dass dafür keine Permission notwendig ist?
  - Frage zu Sicherheit / Privacy, falls bisher nicht erwähnt?
    - sensibel sein, da CASED Leute ;)
    - Wenn erwähnt auch genauer nachfühlen, ob neues **(Gruppen-)System** verstanden / bemerkt wurde?
- Angenommen Sie möchten eine Funktionalität einer App unbedingt, welche **Trade-Offs** würden Sie akzeptieren, d.h. welche Permissions wären für eine gewünschte Funktionalität akzeptabel? Wie entscheiden sie dies?
  - Wenn ich Funktionalität XY unbedingt brauche / möchte, aber Kosten höher sind, wie gehe ich damit um?!
  - Frage zu Permissionsverständnis? … wie genau zu stellen ist noch unklar?! - Hier IMPLIZIT gefragt
- Was sollte im Interface besonders verbessert werden, um die Suche & Auswahl von Apps für den Endkunden / Security-Experten zu verbessern, d.h.
  - **Einfacher** zu machen
  - **Übersichtlicher** zu machen
  - **Sicherer** zu machen
  - **Privatsphäre schützender** zu machen
- **[FALLS INFORMATIK]** Hast du einen QR-Code Scanner installiert … wenn ja welchen? Was war der Grund dafür, dass du genau diesen hast? Hast du die Verteilermail mitbekommen mit dem SecUSo-QR Scanner?
- MOCK UP

A2. Evaluationsstudie des Prototypens

[Zugehöriger Inhalt in Kapitel 3 ab Seite 29]

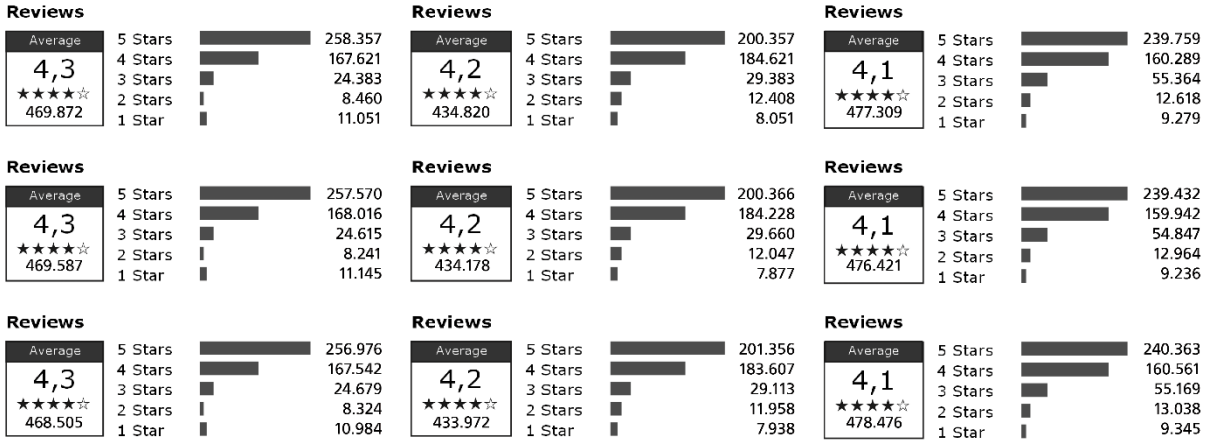

Abbildung 19. Überblick über alle verwendeten Nutzerbewertungsdarstellungen; für jede Entscheidungssituation wurden jeweils drei zufällig ausgewählt

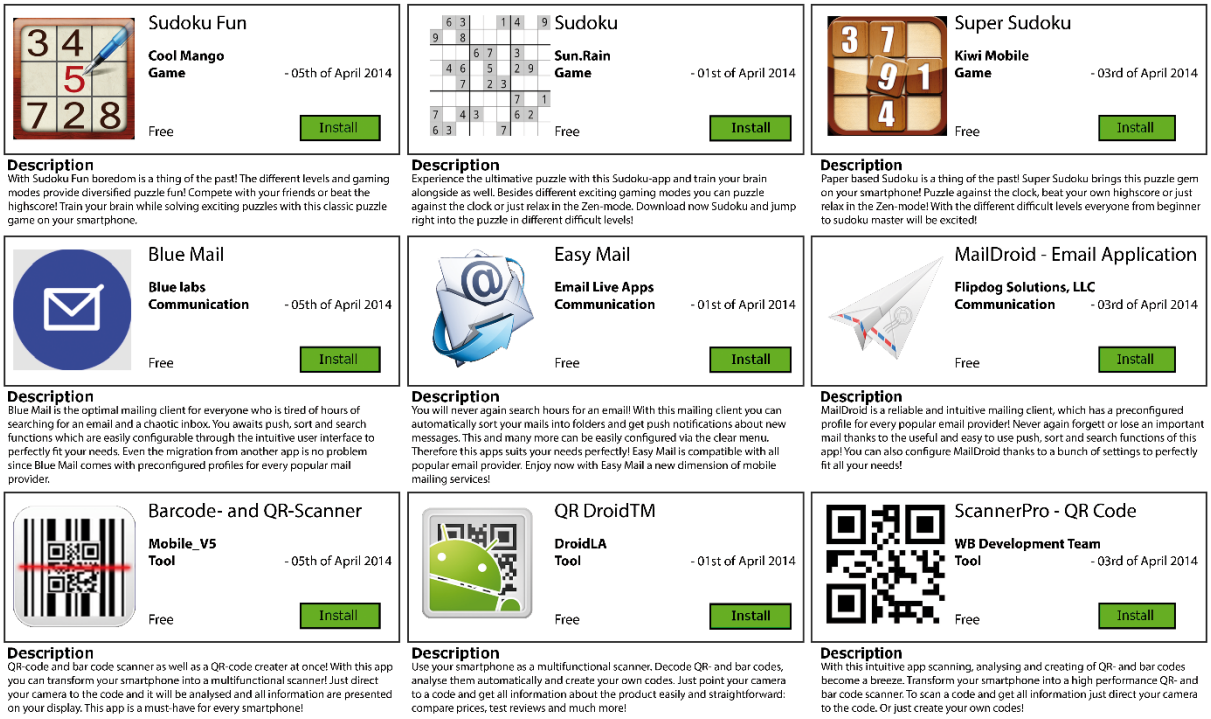

Abbildung 20. Überblick über alle verwendeten Applikationsnamen, Logos, Entwicklernamen sowie Applikations Beschreibungen; die Zuordnung zwischen Applikationsname und -beschreibung war jeweils fixiert, alle anderen Zuordnungen würden für jeden Teilnehmer zufällig ausgewählt

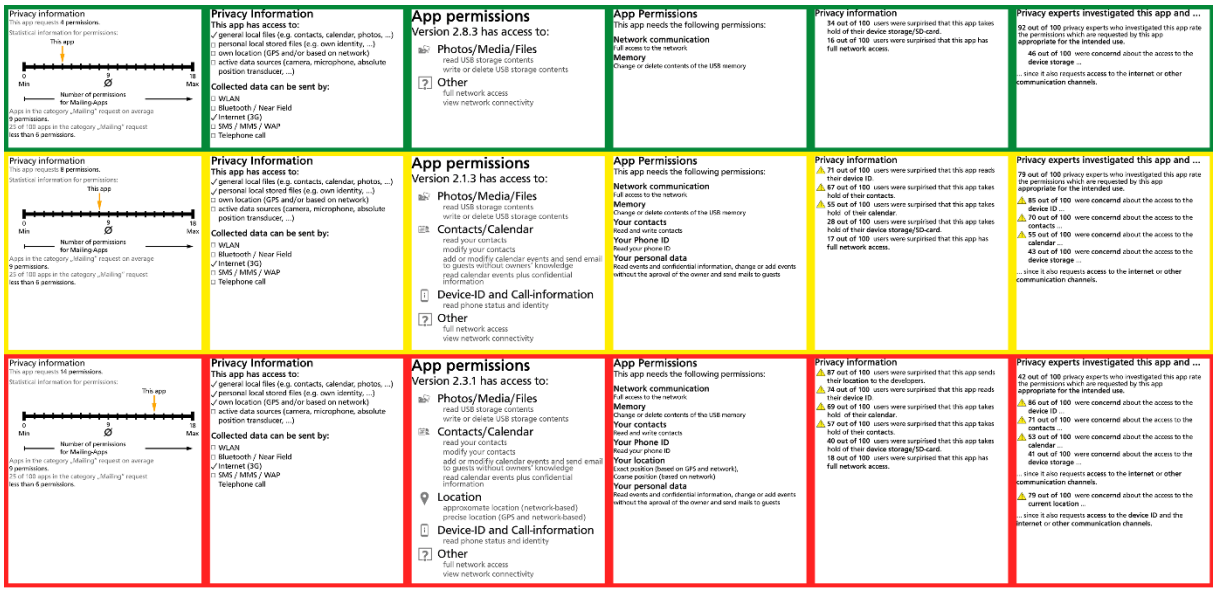

Abbildung 21. Überblick über alle Berechtigungsdarstellungen der verschiedenen Typen für die Applikationskategorie E-Mail, wobei die beste Alternative jeweils in der obersten Reihe (grün), die schlechteste in der untersten Reihe (rot) abgebildet ist; jedem Teilnehmer wurde zu Beginn ein Darstellungstyp (Spalte) zufällig für alle drei Entscheidungssituationen zugeordnet

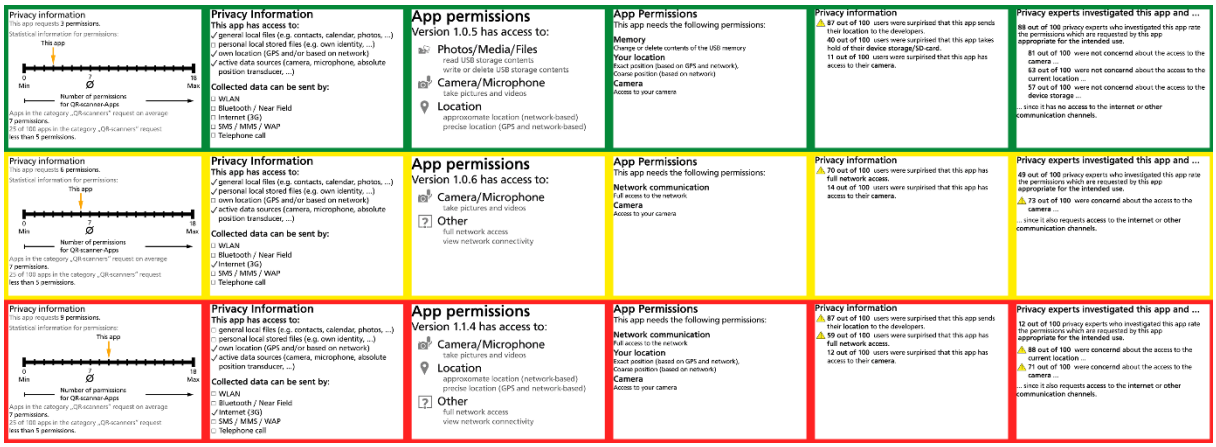

Abbildung 22. Überblick über alle Berechtigungsdarstellungen der verschiedenen Typen für die Applikationskategorie QR-Code-Scanner, wobei die beste Alternative jeweils in der obersten Reihe (grün), die schlechteste in der untersten Reihe (rot) abgebildet ist; jedem Teilnehmer wurde zu Beginn ein Darstellungstyp (Spalte) zufällig für alle drei Entscheidungssituationen zugeordnet

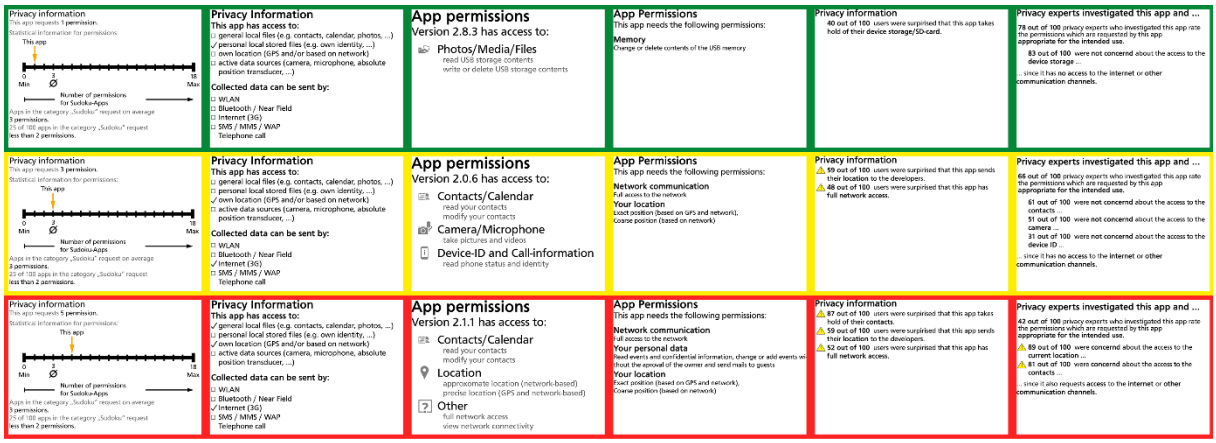

Abbildung 23. Überblick über alle Berechtigungsdarstellungen der verschiedenen Typen für die Applikationskategorie Sudoku, wobei die beste Alternative jeweils in der obersten Reihe (grün), die schlechteste in der untersten Reihe (rot) abgebildet ist; jedem Teilnehmer wurde zu Beginn ein Darstellungstyp (Spalte) zufällig für alle drei Entscheidungssituationen zugeordnet

A3. Studie zum integrativen Verhaltensmodell

[Zugehöriger Inhalt in Kapitel 4 ab Seite 48]

Tabelle 9. Überblick über die Korrelationen zwischen den Konstrukten; auf der Diagonale sind die Quadratwurzeln der durchschnittlich extrahierten Varianzen eingetragen

	FA1	FA2	FA3	FA4	FA5	FA6	FA7	FA8	FA9	FA10	FA11	FA12	FA13	FA14	FA15	FA16	FA17	FA18	FA19	FA20
FA1	**0.84**																			
FA2	0.04	**0.90**																		
FA3	-0.21	-0.10	**0.91**																	
FA4	-0.09	0.03	0.01	**0.75**																
FA5	0.18	0.06	-0.09	-0.02	**0.78**															
FA6	-0.12	-0.12	0.01	-0.01	-0.05	**0.85**														
FA7	0.19	-0.03	0.02	-0.12	0.03	-0.09	**0.87**													
FA8	-0.15	-0.25	0.04	-0.15	-0.06	0.28	-0.04	**0.82**												
FA9	0.05	0.04	0.02	-0.04	0.04	-0.05	0.11	-0.11	**0.96**											
FA10	0.07	0.11	-0.22	-0.03	0.06	0.03	-0.02	-0.05	-0.07	**0.71**										
FA11	-0.08	-0.16	0.15	-0.05	-0.08	0.16	0.05	0.15	-0.01	-0.10	**0.79**									
FA12	0.13	0.23	-0.03	-0.15	-0.02	-0.14	0.06	-0.13	0.03	0.02	-0.05	**0.89**								
FA13	-0.23	0.05	0.21	0.05	-0.16	0.02	0.04	0.09	0.00	-0.09	0.05	-0.04	**0.79**							
FA14	-0.25	-0.13	0.00	0.06	-0.15	0.21	-0.17	0.17	-0.08	0.11	0.03	-0.19	0.06	**0.81**						
FA15	-0.18	-0.09	0.23	0.07	-0.12	0.15	-0.12	0.06	0.03	-0.12	0.19	-0.11	0.19	0.04	**0.75**					
FA16	-0.21	-0.08	0.11	0.14	-0.04	0.24	-0.22	0.17	-0.10	0.01	0.06	-0.21	0.08	0.24	0.14	**0.82**				
FA17	-0.08	-0.08	0.11	0.04	-0.24	0.34	-0.06	0.17	-0.06	0.07	0.13	-0.12	0.11	0.27	0.16	0.43	**0.84**			
FA18	-0.42	0.09	0.21	-0.02	-0.30	0.00	-0.04	0.00	0.02	-0.15	-0.01	0.00	0.31	0.05	0.18	0.02	0.10	**0.85**		
FA19	-0.08	-0.17	0.03	0.07	-0.08	0.05	0.01	-0.03	-0.03	0.12	0.01	-0.06	-0.05	0.01	-0.01	-0.03	-0.02	-0.04	#	
FA20	-0.13	0.01	0.09	0.07	0.02	0.02	-0.16	-0.02	-0.10	0.11	-0.22	-0.02	0.08	0.10	0.03	0.17	0.00	0.06	0.06	#

Tabelle 10. Verwendete Items zur Verhaltensabfrage inklusive prozentualem Anteil der Probanden, die keine Angabe zur entsprechenden Frage machten

Item	Prozent ohne Antwort
What is your age?	0,29
What is your weight in pounds?	2,59
What is your gender?	0,57
What extracurricular activities did you do in school?	15,52
What internships did you do in your life?	16,67
What was your school final grade point average?	12,07
In which federal state do you live?	2,59
How many kids do you have?	2,01
Do you want to have children in the future?	3,74
Do you fart secretly in public?	4,89
How often do you drink alcohol?	2,59
If you drink alcohol, how much do you usually drink (e.g. five beer)?	5,75
Have you ever taken drugs?	2,30
Have you ever cheated on your sexual partner?	0,29
Have you ever been cheated on by your current or a former partner?	0,57
How many different sexual partners did you had?	13,79
Have you ever had unprotected sex outside of relationships?	2,30
Have you ever secretly read your partner's personal messages on his or her cell phone?	1,72
Have you ever had more than one partner at the same time?	1,44
At what age did you have sex for the first time?	11,78
Do you use contraception? If yes, which type of contraceptive method are you using?	7,76
Have you ever tried erotic practices or roleplaying involving bondage, discipline, dominance and submission, sadomasochism, or other related interpersonal dynamics?	7,47
How often do you masturbate per week?	21,26
How often do you have oral sex per week?	16,95
Have you ever masturbated?	6,61
Which are your most favorite sexual positions?	33,62
Do you regularly shave your genital area?	6,32
What is your relationship status?	1,15
Have you ever stolen anything (e.g. in a restaurant or a store)?	1,44
Have you ever busted a parking car and left without leaving your name and address?	1,15
Have you ever broken the speed limit while driving?	2,01
Have you ever deliberately refrained from voting?	1,72
For whom did you vote in the last presidential election?	2,59
Which Religion are you affiliated with?	9,48
What is your parent's annual total income?	9,48
What is your annual income?	4,31
Do you currently have credit card debts?	2,01

How much money do you normally spend on clothes, shoes or bags per month?	9,77
Do you have any allergies?	2,30
Have you ever had to undergo surgery? If yes, which kind of?	2,30
Do you take pharmaceuticals?	4,31
What is your blood type?	2,01
Have you ever received psychiatric treatment?	3,16
Have you ever suffered from a sexually transmitted disease?	2,30
Do one or more members of your family suffer from diabates?	0,86
Do one or more members of your family suffer from any other disease (e.g. cancer or Alzheimer)?	17,82
Please assess to which extent you agree with the following statements. | If you prefer not to anwser one particular question, please choose "no answer" – siebenstufige Likert Skala	
Mister Trump is a good president for the United States of America.	2,30
American jobs are more important than climate change.	1,72
Possession of personal weapons is a necessary right to protect the own family.	2,59
I doubt the holocaust has ever happened.	1,72
I have voted for a political party that would embarrass me if my family and friends knew about it.	1,72
I agree with some parts of the agenda of the Ku-Klux-Klan.	1,15
I think whistleblower like Edward Snowden should receive the death penalty.	2,30
I think Afro-Americans are more likely to be criminal.	0,86
I frequently drive when I am drunk.	0,57
I frequently download films or music illegally.	2,30
If I get too much change, I usually keep it.	2,01
If I find something valuable, I prefer to keep it instead of taking it to the lost and found.	1,44
When I got drunk for the first time, I was younger than 21.	3,16
I believe in god.	1,44
I would say I am a very religious person.	0,29
I don't think the catholic church is a good representation for god itself on earth.	6,90
Praying to god is a very important part of my daily life.	2,01
Since I believe god has created the world, I doubt the Darwinian theory of evolution.	2,30
Abortion should be prohibited.	2,30
Because of my religion, I would only accept a partner with the same beliefs.	2,87
I always try to act morally, since I fear later punishment in hell.	2,87
I believe god routes my fate.	2,30
Sometimes I even lie to my partner.	3,16
I masturbate regularly, even when I'm in a relationship.	6,32
I find bondage gear sexually appealing.	3,16
I think it's okay to have more than 20 sexual partners in life.	4,31
Changing sex partners regularly keeps sex interesting for me.	4,02
I would like to have some a same sex sexual partner.	5,46